

2004

Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes Under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort

Richard C. Turkington
Villanova University School of Law

Follow this and additional works at: <https://digitalcommons.unl.edu/nlr>

Recommended Citation

Richard C. Turkington, *Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes Under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort*, 82 Neb. L. Rev. (2003)
Available at: <https://digitalcommons.unl.edu/nlr/vol82/iss3/4>

This Article is brought to you for free and open access by the Law, College of at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Nebraska Law Review by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes Under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort

TABLE OF CONTENTS

I. Introduction	695
II. Values at Stake in Marital and Custodial Surveillance .	696
A. Countervailing Values	698
B. Some of the Complexities in Accommodating Values in Spousal or Parental Electronic Surveillance Cases	698
1. The Inherent Pervasiveness of Electronic Surveillance	699
2. Parental Autonomy, The Best Interests of the Child, and Minor Autonomy	699
III. Federal and State Wiretap and Stored Communications Acts and the Common Law Privacy Intrusion Tort	700
A. Background on Federal Wiretap Law	700

© Copyright held by the NEBRASKA LAW REVIEW.

* Professor, Villanova University School of Law. The impetus for this article was research done for a presentation at a meeting of the Family Law Section of the American Bar Association. I thank my colleague Lew Becker for inviting me to speak at the meeting and for his many helpful insights on the family law dimensions of the article. Richard Redding was helpful in discussions on minors' rights. A special thanks is owed to Andrew Hart, my research assistant, for his work on the article. Finally, as always, I am grateful for the tireless efforts of my Administrative Assistant, Terri LaVerghetta in preparation of the various drafts of this article.

B.	Enter the 1986 Electronic Communications Act: The ECPA	703
C.	ECPA's Scope and Remedies	704
D.	Recording of Conversations in the Marital Home ...	705
1.	Limited to Spousal Eavesdropping in the Martial Home	706
2.	"Bugging Conversations" in the Marital Home ..	706
E.	Parental Tape Recording of Conversations of Children	706
1.	The Extension Phone Exception	707
2.	Vicarious Consent	708
a.	Limitations on the Vicarious Consent Defense	710
b.	The Test for Parental Motive	710
c.	Critique of the Vicarious Consent Rule	711
i.	The Joint Custody Problem	711
ii.	The Non-Identity of Interest Problem ...	713
iii.	Self-Minimization Under the Vicarious Consent Doctrine	714
d.	The Minimization Problem	715
F.	Silent Video Surveillance	716
G.	The Role of State Law	716
1.	Interspousal Exceptions Under State Law	716
2.	The State Interspousal Tort Immunity Defense ..	717
H.	Interspousal and Parental Access to E-Mail: Title I of the ECPA Off the Table	717
IV.	Title II, The Stored Communications Act Downloading E-mail from Computers Located in the Home	719
A.	Separate E-Mail Accounts and Separate Passwords	719
B.	The "In Electronic Storage" Requirement of Title II	720
C.	<i>White v. White</i> ¹	721
a.	E-Mail Was Not in "Electronic Storage"	722
b.	Unauthorized Use	722
D.	The Interspousal Exception	722
E.	The Privacy Intrusion Tort	723
a.	Invasions of Privacy and Intentional Infliction of Emotional Distress	726
b.	Privacy Intrusion Tort and Silent Video Surveillance	727
c.	Interspousal Access to E-Mail and the Privacy Intrusion Tort	730
V.	Exclusion of Fruits of Illegal Surveillance	732

1. 781 A.2d 85 (N.J. Super Ct. Ch. Div. 2001).

A. The Fault Requirement for Violation of the ECPA . . .	732
B. The Federal Wiretap's Strict Exclusionary Rule	734
C. No Exclusionary Rule Under Title II	735
D. Exclusion of Evidence for Privacy Intrusion Tort Invasions	736
VI. Minimization of Privacy Invasions by Protective Orders in Discovery	737
A. Constitutionally Based Privacy Rights	738
VII. Conclusion	739

I. INTRODUCTION

In domestic disputes, family members, persons in courtship, and sexual partners may be motivated to record telephone conversations or access e-mail or voicemail communications to protect their perceived self-interest or out of spite and anger.² The unauthorized access of the content of conversations or communications in domestic disputes is an invasion of any non-consenting person's privacy. This Article examines whether such invasions of privacy are legally justified.

The full extent of intra-family eavesdropping is not determinable for obvious reasons. Persons generally have no way of knowing whether their conversations are surreptitiously listened to. A successful eavesdropper does so in secret. Even if the invasion of privacy is discovered the victim may be reluctant to come forward because of the potentially embarrassing content of the conversation. Currently, there is no national commitment to study the extent of illegal eavesdropping in the United States. In 1976, however, an important study that reviewed laws relating to electronic surveillance was published.³ It suggested that illegal surveillance in marital and domestic disputes was a significant problem. The study indicated that 79% of the illegal wiretapping reported to the Federal Bureau of Investigation (FBI) for which a motive could be identified involved surveillance by spouses,

2. The term "domestic disputes" is used in this Article to include disputes between those who are married or have a family relationship. The Article does not address the interesting question of whether homosexual or bisexual relationships (where there are no children involved) that have been granted some form of partnership status under law would get the benefit of the exceptions to eavesdropping laws that have been granted to those in a marriage or family relationship.

3. NAT'L COMM'N FOR THE REVIEW OF FED. & STATE LAWS RELATING TO WIRETAPPING AND ELEC. SURVEILLANCE [hereinafter National Commission], ELEC. SURVEILLANCE 160 (1976) [hereinafter the NATIONAL COMMISSION REPORT of 1970]. The Commission was created pursuant to a mandate in Section 804 of the Omnibus Crime Control Act of 1968. Unfortunately there has been no subsequent commissions or other governmental bodies that have updated the data in the national Commission Report of 1976.

parents, or those in courtship.⁴ Many of these illegal surveillances were instituted with the advice of an attorney and the assistance of a private detective.⁵ Clearly electronic surveillance of conversations in marital and custody disputes is not uncommon. The increase in court adjudications of electronic eavesdropping arising from domestic disputes suggests that these activities may be on the rise. It is also clear that spouses are accessing e-mail and tracking computer use in connection with domestic disputes.

The legality of electronic surveillance of conversations and accessing of e-mail is complicated. Several legal institutions are implicated by these activities. Section I of this Article identifies the values that are at stake when electronic surveillance is employed in marriage and custodial disputes. Section II examines the legality of electronic surveillance in domestic disputes under state and federal wiretap and stored communications acts and the common law privacy intrusion tort. Section III examines the extent to which the fruits of violations of wiretap and stored communications acts or the privacy intrusion tort are excluded from divorce and custody proceedings. Section IV examines the availability of protective orders and other legal tools which minimize the scope of legal electronic surveillance and provide some protection against invasions of privacy to innocent participants of conversations or communications that are acquired in legal intra-family surveillance.

II. VALUES AT STAKE IN MARITAL AND CUSTODIAL SURVEILLANCE

Important values are implicated when conversations, communications, and images are surreptitiously tape recorded or videotaped. Conversational privacy is an important form of informational and physical privacy. "Informational privacy" refers to a condition, value, interest, or right that embodies a concern about limiting access to one's personal affairs. Physical privacy is the right to decide who shall have access to a physical space or physical access to one's body. Informational privacy and physical privacy sometimes collapse into each other. Hiding a tape recorder in someone's bedroom invades both informational and physical privacy.⁶

4. *Id.*

5. *See id.* at 161.

6. *See Hamberger v. Eastman*, 206 A.2d 239 (1964). For a more general account of the author's views on informational privacy, see RICHARD C. TURKINGTON & ANITA L. ALLEN, *PRIVACY LAW CASES AND MATERIALS* 77 (2d ed. 2002).

Conversational privacy is valued on both intrinsic and instrumental grounds.⁷ Some commentators and jurists view privacy as a value that is essential to our status as persons with dignity rights. Limiting who has acquaintance with the content of one's conversation is a feature of the dignity that is essential to personhood. An influential voice in explicitly connecting privacy and respect for persons was the philosopher Stanley Benn.⁸ Benn contends that the essence of the wrong that occurs through invasions of privacy from unlicensed observations of someone is lack of respect for the subject as a person. Under this view, surreptitious acquisition of the contents of a conversation is a "blow to human dignity."⁹

In addition to being intrinsically valuable, conversational privacy is also important because it is an instrument for furthering other important values. Expecting that what one says to others is private is essential for entering into and altering personal, intimate, and political associations.¹⁰ As some jurists have observed, "[n]o one talks to a recorder as he talks to a person."¹¹ Moreover, privacy in conversations promotes spontaneous expressions of thoughts and emotions that make it possible for others to know an individual and for that individual to know others. Conversational privacy is also viewed as essential to the formation of self identity and personality. The same arguments and values apply to the importance of privacy in communications like e-mail, which do not involve the human voice.¹²

-
7. For a general account of the various views of privacy as a value that is an intrinsic good and as a value that is instrumentally good because of what privacy does for other important values, see TURKINGTON & ALLEN, *supra* note 6, at 27-29.
 8. See Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in *PRIVACY: NOMOS XIII* 1-26 (J. Roland Pennock & John W. Chapman eds., 1971).
 9. See Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 974 (1964) (characterizing eavesdropping, wiretapping, and the unwanted entry into one's house as a "blow to human dignity"); see also TURKINGTON & ALLEN, *supra* note 6, at 50-51 (providing a general account of the dignity and respect for person foundations of privacy law).
 10. See *United States v. United States Dist. Court for E.D. Mich.*, 407 U.S. 297 (1972) (holding that the President did not have the inherent power to wiretap phones of United States citizens); *Commonwealth v. Blood*, 507 N.E.2d 1029 (Mass. 1987) (noting Massachusetts law prohibits unreasonable searches and seizures violated by electronic surveillance of conversations in the home unless all of the parties have consented); see also *Bartnicki v. Vopper*, 532 U.S. 514, 532 (2001) (recognizing the role of privacy in communications in "uninhibited exchange of ideas" amongst citizens).
 11. See *Blood*, 507 N.E. 2d at 1036 (quoting *Holmes v. Burr*, 486 F.2d 55, 72 (9th Cir. 1973) (Hufstедler, J., dissenting)).
 12. See generally A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395 (1996); Donald J. Karl, *State Regulation of Anonymous Internet Use After ACLU of Georgia v. Miller*, 30 ARIZ. ST. L.J. 513 (1998); TURKINGTON & ALLEN, *supra* note 6, at 450.

A. Countervailing Values

The countervailing values that are asserted to justify encroachments on conversational and communication privacy in marital and custodial electronic surveillance cases are parental autonomy in child rearing, the best interests of the child, and the integrity of the fact finding process in divorce and custody proceedings.

Parental autonomy in decisions involving the rearing and upbringing of their children is a longstanding value in the United States.¹³ Until the age of majority, parents have the authority to decide most decisions for their children. This parental autonomy may include a decision to invade the informational and physical privacy of their children. With minor children legally incapable of consent, parents have autonomy to access their children's health records and consent to physical invasions of privacy through beneficial medical procedures. Parental autonomy in child rearing, however, is not absolute. In some cases parental decisions are overridden where the decision is not in the physical or emotional best interests of the child.¹⁴ The best interests of the child may also override the informational and physical privacy values of the parents. Where a question of physical or sexual abuse has been raised in psychiatric examination of a parent, the privacy and confidentiality of health information gives way to the interest in the physical and psychological well being of the child.¹⁵

B. Some of the Complexities in Accommodating Values in Spousal or Parental Electronic Surveillance Cases

There are several features of parental or spousal electronic surveillance that make the accommodation of values complicated in some cases.

-
13. See *Meyer v. Nebraska*, 262 U.S. 390 (1923) (holding parents have right to control the content of their children's education); *Wisconsin v. Yoder*, 406 U.S. 205 (1972) (holding Wisconsin compulsory public school attendance law interfered with parent's rights to religious expression protected by First Amendment).
 14. One example, which is not the focus of this Article, would be where the child's life could be saved with a blood transfusion, but the parents' religious beliefs forbid the procedure. See, e.g., *State v. Rogers*, 20 P.3d 166, 169 (Okla. Civ. App. 2001) (discussing a compelling interest of a state in preserving the lives of children).
 15. Originally states adopted laws requiring physicians to report suspected physical and sexual abuse to authorities. Today, most states have greatly extended the scope of this duty to mental health professionals. The duty of both physicians and mental health professionals is triggered where there is a reasonable basis for suspicion of abuse. Moreover, some jurisdictions impose criminal liability for a failure to disclose such information to the proper authorities. For a more in depth analysis of the issues surrounding disclosure of confidential communications in psychotherapy, see RICHARD C. TURKINGTON & ROBERT M. WETTSTEIN, *CONFIDENTIALITY LAW AND THE TESTIMONIAL PRIVILEGE IN PSYCHIATRY*, reprinted from *PSYCHIATRY* (Robert Michaels et al. eds., rev. ed 1996/97).

1. *The Inherent Pervasiveness of Electronic Surveillance*

Electronic surveillance through a wiretap or bug¹⁶ is inherently pervasive. A wiretap, bug, or the downloading of a person's e-mail or voicemail breaches the conversational and communication privacy of all non-consenting persons that are talking on the telephone or are a part of the conversation or e-mail communication. Even if there are justifications for invading the privacy of a targeted person the privacy of non-targeted persons is invaded. Persons whose privacy is invaded without justification are innocent victims of the inherent pervasiveness of electronic surveillance technology. Electronic surveillance may provide access to, and extra-judicial disclosure of, highly personal and intimate information of innocent persons. In the sections that follow, this Article will show that the pervasive nature of electronic surveillance is not adequately accounted for in much of the law on electronic surveillance. When adequately taken into account the pervasive nature of electronic surveillance may push the accommodation of values in favor of conversational and communication privacy.

2. *Parental Autonomy, The Best Interests of the Child, and Minor Autonomy*

Parental autonomy to electronically eavesdrop on the conversations or communications of a minor child is limited when the surveillance is not in the best interest of the child or where the surveillance violates the minor's autonomy to communicate. As observed above, the best interests of the child may override parental choices on childrearing and parental informational privacy values. Beyond this there is an emerging tradition in our legal system to grant minors self determination in respect to decisions that have traditionally been left exclusively to parents.¹⁷ Much of the discussion in commentary and law focuses on empirical studies that suggest that minors are competent to make important decisions at ages much earlier than traditional legal ages of majority.¹⁸ Statutes have been enacted in several states providing for "mature minors" to have the right to informed

-
16. A "wiretap" involves acquisition of the contents of a conversation that is transmitted from one point to another in some part by a system involving wires. Intercepting telephone conversations is a classic wiretap. A "bug" involves the use of a transmitter or tape recorder to acquire the contents of face to face conversations.
 17. See Kellie Smidt, *"Who Are You To Say What My Best Interest Is?" Minors' Due Process Rights When Admitted by Parents for Inpatient Mental Health Treatment*, 71 WASH. L. REV. 1187 (1996), for a background on the changing landscape of minors' right to consent for treatment.
 18. See RICHARD E. REDDING, *DUE PROCESS PROTECTIONS FOR JUVENILES IN CIVIL COMMITMENT PROCEEDINGS* 24 (Elissa C. Lichtenstein et al. eds., 1991). For a source of state law that demonstrates the variable ages adopted by legislation for minors' consent, see NATIONAL SURVEY OF STATE LAWS 443-56 (Richard A. Leiter ed., 3d ed. 1999).

consent for medical treatment and psychotherapy.¹⁹ In psychotherapy, the right of a minor's informed consent for treatment is thought by psychotherapists to facilitate mental health treatment.²⁰ The importance of this recent development is that the rigid historic view that parents have autonomy over dependent children until they reach the age of eighteen or twenty-one is being replaced in some states by a flexible view that minors reaching a level of competency have the right to decide certain matters for themselves. This changing landscape of minor autonomy and the limitations on parental autonomy where the best interests of the child are at stake, need to be taken into account in parental electronic eavesdropping cases.

III. FEDERAL AND STATE WIRETAP AND STORED COMMUNICATIONS ACTS AND THE COMMON LAW PRIVACY INTRUSION TORT

The importance of conversational and communication privacy values are reflected in several legal institutions that are brought to bear in parental and spousal electronic surveillances cases. Three of these legal institutions are federal wiretap and stored communications acts, state wiretap and stored communications acts, and the common law privacy intrusion tort.

A. Background on Federal Wiretap Law

The recording of telephone and face-to-face conversations and the accessing of e-mail and voicemail are primarily regulated by federal and state wiretap and stored communications statutes. The federal wiretap statute is notorious for its lack of clarity.²¹ It will be helpful to begin by laying a foundation of the basic concepts and structure of federal law and identifying areas where there is some clarity.

In 1928, the Supreme Court, in *Olmstead v. United States*, held that a government wiretap was not a search under the Fourth Amendment.²² Chief Justice Taft, writing for the majority, concluded there was no search because the electronic device attached to the wire outside of Olmstead's home did not amount to a physical trespass.²³

19. See Tania E. Wright, *A Minor's Right to Consent to Medical Care*, 25 HOWARD L. J. 525, 528-38 (1982) (arguing for drastic legislative reform of minor consent law in view of inconsistent and inadequate common law and legislative rules).

20. See Redding, *supra* note 18, at 18.

21. See *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998) (noting that this characterization by the Fifth Circuit of the federal wiretap statute may have been too generous).

22. 277 U.S. 438 (1928).

23. *Id.* at 464-65. The physical trespass notion of a Fourth Amendment search was junked by the Supreme Court almost forty years later in *Katz v. United States*, 389 U.S. 347 (1967).

The Court did note, however, that the privacy of telephone conversations could be protected by direct legislation.²⁴ Congress responded in 1934 by enacting the Federal Communications Act (FCA).²⁵ Section 604 of the FCA prohibited interception of conversations, but was limited in several ways. Evidence obtained in violation of the FCA could be admitted in state court. In addition, the Justice Department and FBI interpreted § 605 to only prohibit wiretaps that were "divulged."²⁶ Finally, the Supreme Court severely limited application of § 605 in transmission monitoring or "bugging" cases that did not involve wiretapping by imposing a trespass requirement on these forms of electronic eavesdropping.²⁷

In 1967, the Supreme Court junked the trespass concept of a Fourth Amendment search and reversed *Olmstead*.²⁸ In *Katz v. United States*,²⁹ the Court held that electronic surveillance of a conversation by the government constituted a search if the person had a reasonable expectation of privacy in the conversation. This shift from a trespass based notion of a Fourth Amendment search to one based on an individual's expectation of privacy was paradigmatic. *Katz* ushered in the modern era of informational privacy law. As discussed later in this Article, the expectation of privacy principle, as employed by courts since *Katz*, is fraught with problems. Nevertheless, the idea that a legally recognized expectation of privacy is the *sine qua non* for *prima facie* privacy protection permeates informational privacy law in the private and public sector.³⁰

Partially in response to the limited protection provided within § 605 and the emergence of constitutional protection for conversational privacy after *Katz*, Congress enacted the first comprehensive federal statute regulating virtually all forms of electronic surveillance

24. *Id.* at 465-66 (noting that Congress could protect wire communications by making them inadmissible in judicial proceedings).

25. Federal Communications Act of 1934, ch. 652, § 605, 48 Stat. 1103 (1934) (amended by 47 U.S.C. § 605 (1968)).

26. See, e.g., Herbert Brownell, Jr., *The Public Security and Wiretapping*, 39 CORNELL L. REV. 195, 197-99 (1954); John Decker & Joel Handler, *Electronic Surveillance: Standards, Restrictions, and Remedies*, 12 CAL. W. L. REV. 60, 163 (1975).

27. Compare *On Lee v. United States*, 343 U.S. 747, 749-51 (1952) (holding that there was no violation of § 605 where a conversation is recorded by someone who is "wired for sound"), with *Silverman v. United States*, 365 U.S. 505 (1961) (holding that § 605 was not applicable where the government used a foot-long spike microphone to record a conversation).

28. 277 U.S. 438 (1928).

29. 389 U.S. 347 (1967). *Katz* involved the attachment of an electronic transmitter to a telephone booth that Katz was conversing from and is a transmission monitoring case. Earlier during the same term, the Court had assumed that a government wiretap was a Fourth Amendment search in *Berger v. New York*, 388 U.S. 41 (1967) (construing portions of the New York wiretap statute as unconstitutional under the Fourth Amendment).

30. See *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 479 (Cal. 1998).

of conversations. Title III of the Omnibus Crime Control and Safe Street Acts of 1968 nationalized the law of federal, state, and private electronic surveillance of conversations.³¹ This statute was commonly referred to as the "Wiretap Act" or "Title III."

Congress enacted The Wiretap Act with several objectives in mind. The Wiretap Act was designed to establish the authority and standards for government wiretaps for criminal investigations. Concern is expressed in the legislative history that the government's electronic eavesdropping authority should be clarified to respond to the perceived growing threat of organized crime. In addition, The Wiretap Act was enacted for the purpose of protecting private individuals against wiretapping in domestic disputes and to protect against various forms of wiretapping in the business sector. The extension of The Wiretap Act's prohibition against intercepting conversations to "any person,"³² by providing for minimal liquidated damages,³³ a strong exclusionary rule,³⁴ and the right to recover attorneys' fees and court costs for all violations, reflected concern for protecting conversational privacy in the private sphere.³⁵

The Wiretap Act only protected conversational privacy. This limitation was contained in the prohibition against interception of "wire or oral" communications. Wire communications were those communications involving the human voice that were transmitted from the point of origin to the point of reception through the use of wire.³⁶ Conversing on the telephone is the paradigm of a "wire communication." Face-to-face conversations are the paradigm of an "oral communication." A wiretap is the paradigm of an interception of a wire communication; bugging a conversation through a tape recorder or transmitter is the paradigm of interception of an oral communication. The Wiretap Act generally prohibited the interception of a wire or oral communication without a court order³⁷ unless one of the parties has consented.³⁸

31. See generally Jeremiah Courtney, *Electronic Eavesdropping, Wiretapping and Your Right to Privacy*, 26 FED. COMM. B.J. 1 (1973); JAMES G. CARR & PATRICIA L. BELLIA, *THE LAW OF ELECTRONIC SURVEILLANCE* (West 2001).

32. See 18 U.S.C. § 2511(1) (2000).

33. 18 U.S.C. § 2520 (2000).

34. 18 U.S.C. § 2515 (2000).

35. 18 U.S.C. § 2520 (2000).

36. The 1968 version of the Wiretap Act restricted wire communications to those transmitted by telephone companies licensed by the FCC. Wiretap Act, tit. III, § 2510, 82 Stat. 197 (1968).

37. Court ordered surveillance is limited to law enforcement bugs or wiretaps. Section 2518 establishes strict requirements for court authorized interceptions of wire communications. 18 U.S.C. § 2518 (2000).

38. 18 U.S.C. §§ 2511(2)(c)-(d) (2000) (containing consent defenses).

B. Enter the 1986 Electronic Communications Act: The ECPA

In 1986, the federal statute was amended by The Electronics Communications Privacy Act (ECPA).³⁹ Congress enacted The Wiretap Act in 1968 to deal with the then current issues facing privacy law. Title III was directed at the existing technology for electronic surveillance of communications. This consisted primarily of wiretaps and small recorders or transmitters placed upon a person in the place where the communication occurred. During the decades following the passage of The Wiretap Act, however, communication technology changed dramatically. By 1986, many communications were transmitted by means other than the telephone or face-to-face conversations and by systems owned and managed by entities that were not licensed common carriers. Today, many conversations are transmitted by radio signals through cellular systems or cordless phones. In addition, many companies have private phone systems that they tie into the systems of common carriers. There is increasing use of digital technology to electronically communicate through electronic mail and facsimile machines.

The amendments to the Wiretap Act, which resulted from the 1986 passage of the ECPA, responded to the technological advances that had developed since 1968. The response to the new technology is embodied in the addition of the concept of "electronic communication" to the statute.⁴⁰ The ECPA generally prohibits the interception of, and unauthorized access to, stored electronic communications. This addition brings the surveillance of digitally transmitted conversations, electronic mail, cellular phones, and pen registers within the regulatory reach of the statute. While the ECPA restructured and extended federal law in important ways,⁴¹ the 1986 amendments also added to the confusion surrounding the Wiretap Act. The ECPA Amendments now divide the Wiretap Act into Title I, II, and III. The former Title III is now Title I of the ECPA.⁴² Title I⁴³ of the ECPA now regulates the interception of conversations. Title II⁴⁴ of the ECPA regulates access to e-mail, fax communications, and voicemail. Title III⁴⁵ of the ECPA regulates call-tracing devices such as caller ID. The two titles most relevant to this discussion are Title I and Title II. This Article

39. 18 U.S.C. §§ 2510-3127 (1994).

40. See COMMITTEE ON THE JUDICIARY, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, H.R. REP. NO. 99-647, at 2 (1986).

41. For a general analysis of restructuring of the Wiretap Act by the ECPA, see TURKINGTON & ALLEN, *supra* note 6, at 294.

42. Out of habit, some courts and commentators continue to speak of the federal statute as "Title III." This is not technically correct.

43. 18 U.S.C. §§ 2510-2522 (2000).

44. 18 U.S.C. §§ 2701-2711 (2000).

45. 18 U.S.C. §§ 3121-3127 (2000).

will refer to Title I as the "Wiretap Act" and Title II as the "Stored Communications Act".⁴⁶

C. ECPA's Scope and Remedies

The Wiretap and Stored Communications Acts apply to both government and private action. The Wiretap Act imposes criminal and civil liability for intentional interceptions of conversations in violation of the statute.⁴⁷ The Wiretap Act provides for recovery of both actual and punitive damages.⁴⁸ In addition, minimal liquidated damages of \$10,000 may be imposed for violations of the Wiretap Act.⁴⁹ Moreover, the Wiretap Act also contains a strong exclusionary rule prohibiting courts and administrative agencies from admitting into evidence the content of taped conversations that are acquired in violation of the statute.⁵⁰ Attorneys' fees and court costs are also available to the prevailing party.

There are important differences in the scope of regulations and remedies under the Wiretap Act and the Stored Communications Act. Similar to the Wiretap Act, the Stored Communications Act applies to both government and private action as well as providing actual and punitive damages, but the liquidated damages are less; only \$1,000,⁵¹ and most importantly, however, there is *not an exclusionary rule* for violations of Stored Communications Act.⁵² The requirements for court ordered surveillance under the Wiretap Act are stricter than what is required for court ordered access to stored electronic communications under the Stored Communications Act. Both the Wiretap Act and the Stored Communications Act of the ECPA preempt state laws that provide less security for conversations and electronic communications, but state laws can provide for greater security. For example, if one party consents to the recording of a conversation there is

46. See generally TURKINGTON & ALLEN, *supra* note 6, at 294-397.

47. 18 U.S.C. § 2511 (2000).

48. State statutes have similar damage rules. See, e.g., M.G. v. J.C., 603 A.2d 990 (N.J. Super. Ct. Ch. Div. 1992) (upholding \$50,000 punitive damage award against husband for violation of the New Jersey Wiretapping Act).

49. 18 U.S.C. § 2520 (2000). The minimum liquidated damage amount was changed in 1986 (with the ECPA amendments) from \$1,000 to \$10,000. Language in § 2520 was changed from "shall be entitled to damages" to a court "may" assess damages. Most courts have viewed the change to mean that awarding damages is discretionary and that damages should not be awarded for *de minimis* violations of the Wiretap Act. See *Goodspeed v. Harman*, 39 F. Supp. 2d 787, 791 (N.D. Tex. 1999).

50. 18 U.S.C. § 2515 (2000).

51. 18 U.S.C. § 2707(c) (2000).

52. No exclusionary rule is specifically found in Title II. Section 2708 states that "remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708 (2000).

no violation of Title I of the ECPA. In states like Florida,⁵³ Pennsylvania,⁵⁴ Maryland,⁵⁵ and California,⁵⁶ however, both parties must consent for the recording of a conversation by private parties to be legal under the applicable state wiretap law.

D. Recording of Conversations in the Marital Home

As noted above, telephone conversations, including those communicated over cell phones, are "wire communications" under the Wiretap Act. The Wiretap Act specifically prohibits "any person" from intercepting a wire communication without a court order or the consent of one of the parties to the conversation.⁵⁷ Despite the absence of any express exception in the Wiretap Act for the nonconsensual tape recording by one spouse of another spouse's conversation, some courts have carved out a limited exception for interspousal taping of telephone conversations in the marital home. This exception is sometimes referred to by commentators as the "interspousal" or "marital/domestic" conflict exception to the Wiretap Act.

In 1974, the Fifth Circuit Court of Appeals exempted some interspousal electronic surveillance from the Federal Wiretap Act. In *Simpson v. Simpson*⁵⁸, the court held that the recording of telephone conversations in the marital home by a husband who suspected his wife of infidelity did not violate the Wiretap Act. The plain language of the Wiretap Act does not provide for an interspousal/marital conflict exception. Section 2511 imposes criminal or civil responsibility on "any person" who willfully intercepts a telephone conversation. The *Simpson* court, however, found an implied exception for interspousal wiretapping on the basis that Congress did not intend for the Wiretap Act to be thrust into marital controversies or to override state interspousal tort immunity. The court also found that the exception in the statute for ordinary use of an extension phone by the subscriber supported excluding spousal eavesdropping from coverage of the Wiretap Act.⁵⁹ *Simpson* has been followed in only one other federal circuit.⁶⁰ Most of the federal circuits follow the plain language of the ECPA and have not recognized an interspousal exception for wiretapping in the marital home.⁶¹ The majority of courts have also inter-

53. FLA. STAT. ANN. § 934.03(3)(d) (West 2000).

54. 18 PA. CONS. STAT. ANN. § 5704(4) (West 1983 & Supp. 1998).

55. MD. CODE ANN., CTS. & JUD. PROC. § 10-402(C)(3) (1998).

56. CAL. PENAL CODE § 631(a) (West 1998 & Supp. 1998).

57. 18 U.S.C. §§ 2511, 2511(2)(d) (2000).

58. 490 F.2d 803 (5th Cir. 1974).

59. The ordinary use of an extension phone exemption is examined more fully in the section on parental eavesdropping that follows.

60. See *Anonymous v. Anonymous*, 558 F.2d 677 (2d Cir. 1977).

61. See *Heggy v. Heggy*, 944 F.2d 1537 (10th Cir. 1991); *Kempf v. Kempf*, 868 F.2d 970 (8th Cir. 1989); *Pritchard v. Pritchard*, 732 F.2d 372 (4th Cir. 1984); *United*

puted state wiretap acts to not include an interspousal exception for wiretapping in the marital home.⁶²

1. *Limited to Spousal Eavesdropping in the Marital Home*

In those jurisdictions where an interspousal exception has been recognized the exception has been limited to eavesdropping by the spouse in the marital home.⁶³ Persons who assist the spouse in eavesdropping in the marital home, such as a private detective, are liable under Title I even though the spouse is not.⁶⁴

2. *"Bugging Conversations" in the Marital Home*

Face-to-face conversations are "oral communications" under the Wiretap Act. Therefore, the placing of a recording device, commonly referred to as a "bug", in a room or on a person for the purpose of recording face-to-face conversations is subject to regulation under the Wiretap Act as an interception of an oral communication. Where the recording device is used to record the face-to-face conversations of a spouse and another adult in the marital home the result would be identical to the recording of a telephone conversation. If the jurisdiction recognizes an interspousal exception, it would apply to the bugging as well. If there was no recognized exception, the bugging would be illegal. As explained in the section that follows, the wiretapping and bugging of a conversation of a parent/child conversation is subject to a somewhat different analysis.

E. Parental Tape Recording of Conversations of Children

The parental tape recording of conversations between a child and a third party, generally the other parent, is not uncommon where there

States v. Jones, 542 F.2d 661 (6th Cir. 1976). The Eleventh Circuit is the latest court to reject the exception for interspousal wiretapping within the marital home. See Glazner v. Glazner, 347 F.3d 1212 (11th Cir. 2003). Sitting *en banc* all of the members of the court rejected the Fifth Circuit's reasoning in *Simpson v. Simpson*. A majority of the court held that the decision should be applied retroactively in civic cases. Judge Dubina dissented on the retroactive question.

62. See Carr, *supra* note 31, § 3.64, at 3-172 to 3-173 & n.25. One state wiretap act, however, has been interpreted to contain an interspousal wiretap exception. Wright v. Stanley, 700 So. 2d 274 (Miss. 1997).

63. See *Anonymous*, 558 F.2d at 679 (distinguishing Sixth Circuit case where spouse no longer resided in marital home); *Simpson*, 490 F.2d at 809 (noting Title I reflects "Congress's intention to abjure from deciding a very intimate question of familial relations, that of the extent of privacy family members may expect within the home vis-a-vis each other").

64. See *Simpson*, 490 F.2d at 808-09 (noting others may still be liable even if spouse is not).

is a custody dispute.⁶⁵ In such cases, the taping is regarded as more permissible under federal and state wiretap laws. This is due to courts' propensity to treat the recording as within the ordinary extension use exception to the wiretap statute or view the parent as having authority to vicariously consent for the child.

1. *The Extension Phone Exception*

The Wiretap Act contains a narrow exception for electronic eavesdropping over an extension phone that is done for the ordinary use of the subscriber. The ordinary use exception has arisen mostly in cases where an employer records the conversations of employees on an extension phone.⁶⁶ Some courts, due to testimony in the legislative history of the Wiretap Act, have applied the doctrine in cases involving custodial parents recording the conversations of their children. In hearings before the House Judiciary Committee on the scope of the ordinary use exception to the Wiretap Act, Professor Herman Schwartz, speaking on behalf of the ACLU stated, "I take it nobody wants to make it a crime for a father to listen in on his teenage daughter"⁶⁷ This language has been invoked by courts to support a parental eavesdropping exception under federal and state statutes for recording conversations on the extension phone of a child in the family home.⁶⁸

Recognition of a marital conflict and parental extension phone exception for electronic surveillance under the Wiretap Act has been limited and subject to considerable critical commentary.⁶⁹ The marital conflict exception is distinctly a minority rule and has been roundly criticized as unwarranted in view of the plain language and legislative history of the Wiretap Act.⁷⁰ Most state courts have not recognized a

65. See Jonathan E. Niemeyer, Note, *All in the Family: Interspousal and Parental Wiretapping Under Title III of the Omnibus Crime Act*, 81 Ky. L.J. 237, 247 (1993).

66. See, e.g., *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992) (holding employer liable for recording employee's telephone conversations on an extension phone because recording exceeded narrow scope of ordinary business use of extension phone exception). The ordinary course of business exception is found in § 2510(5)(a)(i) which exempts electronic surveillance "by the subscriber or user in the ordinary course of its business" from regulation under Title I of the ECPA. *Id.* at 1157 (noting the source of extension phone exception).

67. *Hearings on the Anti-Crime Program Before Subcomm. No. 5 of the House Comm. on the Judiciary*, 90th Cong., 1st Sess. 901 (1967).

68. See *Scheib v. Grant*, 22 F.3d 149, 154 (7th Cir. 1994); *Newcomb v. Ingle*, 944 F.2d 1534, 1536 n.5 (10th Cir. 1991); *Anonymous*, 558 F.2d at 679.

69. For a general criticism of the marital and parental exception, see Carr, *supra* note 31, § 3.64, at 3-615.

70. *Id.* A thorough trashing of the arguments of the *Simpson* court is found in Judge Celebrezze's opinion in *United States v. Jones*, 542 F.2d 661 (6th Cir. 1976). See discussion *supra* text accompanying notes 58-64. See also the arguments of the court in *Kratz v. Kratz*, 477 F. Supp. 463 (E.D. Pa. 1979). Both decisions find the

marital conflict exception.⁷¹ Many courts have also rejected the telephone extension exception as applied to the tape recording of conversations.⁷²

A potentially much broader exception, however, has recently been recognized by courts that reject both the marital and telephone extension phone exceptions.⁷³ This new exception would authorize parental electronic eavesdropping by granting a parent the authority to vicariously consent for a minor child and thereby provide a defense to the Federal Wiretap Act and those state wiretap acts that allow for electronic surveillance of conversations if one party has consented.

2. Vicarious Consent

The Wiretap Act is not violated if a party to the intercepted conversation has consented. This one party consent rule is mirrored in most state wiretap statutes. Parents and guardians of minors have the authority to vicariously consent for the minor when it is perceived by the parent to be in the best interests of the child. Does the parental authority to consent for the child under state law include consenting to the surreptitious recording of a conversation between the child and a third person? If state law allows a parent to vicariously consent for their child in respect to decisions such as whether to be subject to a particular medical procedure, does that authority provide a consent defense under The Wiretap Act? Does the authority for a parent to consent for the child under state law include consenting to the surreptitious recording of a conversation between a child and the other parent? Courts have generally answered both of these questions affirmatively and have been increasingly willing to apply a vicarious consent defense to parental eavesdropping.

The Tenth Circuit was the first federal court of appeals to suggest vicarious consent was a defense under the Wiretap Act in *Thompson v. Dulaney*.⁷⁴ During the pendency of a divorce, Denise Dulaney taped several conversations between the father and their minor children while she and her children were living in her parents' home.⁷⁵ Dulaney had the tapes transcribed and distributed them to her family, attorney, and expert witnesses.⁷⁶ Two of the transcripts were admitted in the deposition of an expert witness during the custody litiga-

analysis of Judge Bell in *Simpson v. Simpson* to be without support in the language, legislative history, or purposes of the Wiretap Act.

71. See *infra* notes 106-07 and accompanying text.

72. See, e.g., *Thompson v. Dulaney*, 970 F.2d 744 (10th Cir. 1992); *Pollock v. Pollock*, 154 F.3d 603 (6th Cir. 1998).

73. *Pollock*, 154 F.3d at 610.

74. 970 F.2d 744 (10th Cir. 1992).

75. *Id.* at 746.

76. *Id.*

tion.⁷⁷ Thompson, the father, brought a damage action under the Wiretap Act against his wife and his wife's parents, experts, and attorney for taping and divulging the contents of recorded conversations between himself and his children.⁷⁸

The district court exempted the recordings under the interspousal exception.⁷⁹ The Tenth Circuit, in an earlier case, had rejected the view that there was an interspousal exception to The Wiretap Act and reversed the district court on this issue.⁸⁰ The court remanded the case to the district court, however, to determine whether consent was a defense to the Wiretap Act action on the basis that the custodial parent had the authority to vicariously consent for the child under state law.⁸¹ On remand, the district court found that the mother, as guardian of the child, had the right under state law to act on behalf of the child, where to do so was in the child's best interest.⁸² Therefore, in order to fulfill her responsibilities as guardian, the mother could consent for the child under The Wiretap Act if she had "a good faith basis that is objectively reasonable for believing that it is necessary to consent on behalf of her minor children to the taping of the phone conversations"⁸³

Most federal and state courts that have considered the issue have applied a version of the vicarious consent doctrine in parental eavesdropping cases.⁸⁴ The doctrine has been applied to parental eavesdropping on conversations between the other parent and their minor children and third parties such as a babysitter.⁸⁵

77. *Id.* at 746-47.

78. *Id.* at 746.

79. *Id.*

80. *Id.* at 747.

81. *Id.* at 749.

82. *Thompson v. Dulaney*, 838 F. Supp. 1535, 1544 (D. Utah 1993).

83. *Id.* at 1544.

84. *See id.*; *Pollock v. Pollock*, 154 F.3d 601 (6th Cir. 1998); *Campbell v. Price*, 2 F. Supp. 2d 1186 (E.D. Ark. 1998); *Silas v. Silas*, 680 So. 2d 368 (Ala. Civ. App. 1996) (adopting the vicarious consent doctrine in interpreting state wiretap acts); *State v. Diaz*, 706 A.2d 264 (N.J. Super. App. Ct. Div. 1998) (adopting the vicarious consent doctrine in interpreting state wiretap acts); *W. Va. Dep't of Health and Human Res. ex rel Wright v. David L.*, 453 S.E.2d 646 (W. Va. 1994) (interpreting both the state and federal wiretap acts to include the vicarious consent doctrine, while holding those provisions inapplicable in light of the specific facts of the case). Currently, the only court to reject the vicarious consent doctrine has been *Williams v. Williams*, 581 N.W.2d 1777 (Mich. 1998) (interpreting both the Michigan and federal wiretap acts to not recognize vicarious consent in parental eavesdropping cases).

85. *See Diaz*, 706 A.2d at 270 (upholding the admissibility of the audio portion of a video tape in a criminal trial of babysitter for abuse of the child).

a. Limitations on the Vicarious Consent Defense

The availability of the vicarious consent defense is fact specific. The age of the minor and the purpose of the surveillance are factors that are taken into account by courts. A leading case illustrating this is *Pollock v. Pollock*.⁸⁶ Samuel Pollock (Samuel) and his current wife Laura Pollock (Laura) brought a damage action under the Wiretap Act against Samuel's former wife, Sandra Pollock (Sandra), and her two attorneys for tape recording and disclosing the contents of conversations between fourteen year old Courtney Pollock (Courtney) and Samuel and Laura.⁸⁷ The recordings occurred on an extension phone in Sandra's home while Courtney was residing with her.⁸⁸ The district court entered summary judgment for the defendants.⁸⁹ On appeal, the Sixth Circuit affirmed the district court's adoption of the vicarious consent defense under the Wiretap Act, but remanded the case to determine whether Sandra's purpose in taping the conversations was sufficient to preserve the consent defense.⁹⁰ The record contained conflicting evidence as to whether her motive in taping was out of genuine concern for the best interest of the child.⁹¹ If Laura's motivation in taping was to "gain access to Courtney's attorney-client communications" or if in some other sense was not motivated by the best interest of the child, the defense of vicarious consent would not be available.⁹² Where evidence is disputed, motive presents a question of fact that is sufficient to overcome a motion for summary judgment.⁹³

b. The Test for Parental Motive

As suggested by the Sixth Circuit Court of Appeals in *Pollock*, the parent's motive in wiretapping or bugging a child's conversation is crucial to the vicarious consent defense. The test adopted by *Pollock* and other courts⁹⁴ is whether the parent had a "good faith, objectively reasonable basis for believing such consent was necessary for the wel-

86. 154 F.3d 601(6th Cir. 1998).

87. *Id.* at 603 (noting facts surrounding the appeal). Sandra's attorneys, who were named as defendants, were Oliver Barber and Luann Glidewell. *Id.*

88. *Id.* at 604 (noting Sandra's admission to recording phone calls on an extension phone in her home).

89. *Id.* at 605.

90. *Id.* at 610-13.

91. *Id.* at 612-13 (noting "the question of material fact as to Sandra's motives").

92. *Id.* at 611.

93. See *Kroh v. Kroh*, 567 S.E.2d 760, 764 (N.C. Ct. App. 2002) (stating that an issue of fact concerning a defendant parent's motivations for recording was sufficient to preclude summary judgment).

94. *Pollock* adopts the test first articulated in *Thompson v. Dulaney*, 838 F. Supp. 1535 (D. Utah 1993).

fare of the child.”⁹⁵ At least one other state, Alabama, has adopted a stricter version of the parental motive test. Under this standard, the parent must demonstrate a good faith, objectively reasonable belief “that the minor child is being abused, threatened, or intimidated by the other parent.”⁹⁶

c. Critique of the Vicarious Consent Rule

Given the reluctance of courts to sanction spousal eavesdropping under the Wiretap Act for the reasons stated above, it is surprising that the vicarious consent notion has been received favorably by courts without critical examination. This section of the Article will demonstrate that the vicarious consent doctrine should not be recognized under the Wiretap Act. Some of the problems created by recognition of a parent’s right to consent to eavesdropping on a child’s conversations with the other parent and third parties are: (1) the joint custody problem; (2) the non-identity of interests problem; and (3) the minimization problem.

i. The Joint Custody Problem

One of the assumptions of the vicarious consent principle is that authority to consent for the minor child under state law is incorporated into the one party consent defense under state and federal wiretap acts. This assumption ignores the rudimentary features of the important development of joint custody that is recognized in most states.⁹⁷

The traditional model of custody was to grant one parent, usually the mother, both legal custody and physical custody. Legal custody entails the authority to make important decisions involving the upbringing of the child such as where to go to school and whether to be treated medically. Physical custody entails decisions about where the child shall reside and physical care. The traditional model of sole custody grants the custodial parent both legal and physical custody. Non-custodial parents were given visitation rights.

Joint custody was recognized initially by California in 1980.⁹⁸ Joint custody changes the division of responsibility that attached under the traditional sole custody rule. With joint custody, one parent generally has physical custody but both parents share the responsibility for legal custody. A leading commentator indicates that most often

95. *Pollock*, 154 F.3d at 610 (noting adoption of *Thompson* standard of vicarious consent).

96. *Silas v. Silas*, 680 So. 2d 368, 371 (Ala. Civ. App. 1996).

97. See D. KELLY WEISBERG & SUSAN FRELICH APPLETON, *MODERN FAMILY LAW: CASES & MATERIALS* 844 (2d ed. 2002).

98. Some commentators suggest that the father’s rights movement was an important influence in the development of joint custody. *Id.* at 844-45.

in joint custody arrangements, the child's care, education, religion, medical treatment, and general welfare⁹⁹ are shared by both parents. If this form of joint custody under state law applies to the parents in a vicarious consent eavesdropping case, the notion that the state law gives one parent the sole authority to consent to the invasion of privacy of the minor child and the other parent makes no sense. If the authority to vicarious consent is shared by both parents under state law, then that state law is no warrant for the authority of one party to consent for the child under state or federal wiretap acts. If the authority to wiretap is shared, then vicarious consent to wiretap the conversation of a non-physical custodial parent would only be warranted in the unlikely case where that parent agrees to it.

There is virtually no discussion of the impact of the multiple kinds of joint custody arrangements under state law on vicarious consent to wiretapping under wiretap acts. In *West Virginia ex rel. Wright v. David L.*,¹⁰⁰ the court of appeals in West Virginia suggested that the vicarious consent doctrine is limited to the physical custodial parent. David was separated from his wife, Lisa, who was given temporary custody of their twin daughters, Chelsea and Ashley, ages 6, and their son, Joshua, age 5.¹⁰¹ Lisa lived with the children in the marital home. Prior to their divorce David asked his mother to place a voice activated tape recorder in the children's bedroom while she babysat for them.¹⁰²

After listening to these taped conversations, David gave the tapes to his lawyer. The tapes were played to a therapist for Family Services, Inc. and a child protective service worker for the West Virginia Department of Health and Human Resources, and thereafter, David was given physical custody of the children.¹⁰³ In reviewing whether the tape recordings were legal under West Virginia law, the court assumed that the vicarious consent principle applied to the state eavesdropping statute, but held that vicarious consent could not be exercised by a parent with respect to conversations taking place in the home of the parent with physical custody over the child.¹⁰⁴ Therefore, the recording violated the Wiretap Act and was not admissible in the custody proceedings.

It seems odd to vest exclusive authority to the physical custodial parent to decide whether to invade the privacy of the minor child and the non-physical custodial parent when the non-physical parent has

99. See Harold Homer Clark, Jr., *The Law of Domestic Relations in the United States*, § 20.2, 482 (2d ed. 1988).

100. 453 S.E.2d 646 (W. Va. 1994).

101. *Id.* at 648.

102. *Id.*

103. *Id.*

104. *Id.* at 654.

joint decisional authority to consent for the minor. In *Wright*, the physical custodial parent had consented to physical access to the children by the paternal grandparent and her exclusive authority to decide physical access is preserved. Perhaps, the *Wright* decision is palatable if the conversation with the child is viewed as a form of physical custody. That is not a sensible interpretation of physical custody in a case like *Wright*. The non-physical custodial parent had the right to converse over the telephone in *Wright*, and therefore, Lisa Wright's physical custodial authority did not extend to physical access to the children through conversing over the telephone with the other parent. There might be a good argument for viewing taping of a child's conversation with a parent as part of the authority of a physical custodial parent in the rare and exceptional cases where the non-physical custodial parent has been restrained by a court order from conversing over the telephone with a child. In that case, however, the authority to wiretap ought to be pursuant to a court authorization to determine whether the order not to converse with the minor has been violated. The conceptual incomprehensibility of the vicarious consent principle in cases where the parents have joint decisional custody should be, by itself, enough for courts to reject the vicarious consent principle, but there are additional problems that also should move courts in that direction.

ii. *The Non-Identity of Interest Problem*

Even in a perfect family life, the substituted judgment by a parent for the decision of a child may not be identical to the best interests of the child. As Gerald P. Koocher has noted:

The concept of substituted judgment [in which an adult provides a kind of proxy consent] presumes a great deal. Most notably, it assumes that the person making the decision is willing and able to act in this capacity on the child's best interests (i.e., without a conflict of interests). Even within the loving, intact, two-parent family, not all parental decisions regarding children are without conflicts of interest. Parents often subordinate their needs and preferences to the best interests of their children (or to what they believe to be their children's best interests), but this is not always the case.¹⁰⁵

David J. Anderman further observed in a 1993 article:

In the majority of parental wiretapping cases reported, however, the family unit has fallen apart or seems to be deteriorating. Indeed, in only one of the cases involving parental wiretapping were the parents of the child not divorced or seeking a divorce. The interceptions were not effected for the inter-

105. See Gerald O. Koocher, *Children Under Law: The Paradigm of Consent*, in *REFORMING THE LAW: IMPACT OF CHILD DEVELOPMENT RESEARCH* 3, 14 (Gary B. Melton ed., 1987) (citations omitted).

ests of the child, but to give the parent leverage in the settlement of custody battles.¹⁰⁶

The risk that a parent's substituted judgment will not be in the best interest of the child is exacerbated in cases where the family is conflicted by a separation, divorce, or custody fight. In such cases, there is a greater likelihood of a non-identity of interest between the parent's choice and the child's best interest. A decision of a parent in a marital or custodial dispute, to wiretap or bug the conversations of a child with the other parent, is rife with the risk of non-identity of interest – that the eavesdropping parent is motivated by personal interest or hostile motive against the other parent and not by the best interests of the child.

Is the increased risk of non-identity of interests in parental electronic surveillance cases adequately accounted for, or protected against in courts adoption of the substituted consent doctrine? Given the limitations of the self-minimization rule of vicarious consent, the increased risks of non-identity of interests are not adequately accounted for.

iii. Self-Minimization Under the Vicarious Consent Doctrine

A wiretap on a telephone line records the conversations of all of the parties that are talking. Even if there is justification for recording conversations between targeted parties, the pervasive nature of a wiretap is such that the privacy of parties, for whom there is no justification, is invaded. Recording portions of the conversation between targeted parties may not be justified because they are not relevant to the legitimate purposes of the eavesdropping. The privacy invasiveness of a wiretap led Justice Douglas to describe a wiretap as:

[A] dragnet, sweeping in all conversations within its scope – without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate conversations.¹⁰⁷

Court ordered wiretaps under The Wiretap Act impose an obligation on the government to minimize the interception of conversations that are not evidence of criminal conduct.¹⁰⁸ One of the problems with exceptions to the Wiretap Act in private surveillance cases is the absence of any court review to determine whether efforts were made to minimize the overreach of the wiretap or bugging.

106. David J. Anderman, *Title III At A Crossroads: The Ordinary Course of Business in the Home, The Consent of Children, and Parental Wiretapping* 141 U. PENN. L. REV. 2261, 2290 (1993).

107. *Berger v. New York*, 388 U.S. 41, 65 (1967) (Douglas, J., concurring).

108. See 18 U.S.C. § 2518(5) (2000) (setting forth a variety of limitations in the hopes of minimizing the scope of unnecessary privacy invasions).

d. The Minimization Problem

The courts that recognize a vicarious consent defense to The Wiretap Act in parental eavesdropping cases contemplate self-minimization by the parents and/or their lawyer if the lawyer has advised them of the legality of wiretapping or bugging a child's conversations. The self-minimization obligation is implicit in the limitation of the vicarious consent authority to eavesdropping where the parent is properly motivated. Under either the strict or loose sense of proper motivation that is discussed above, it would not be legal for a parent to wiretap or bug conversations between their child and a third person if the purpose was simply to gather evidence for prospective or pending custody or divorce litigation. The proper motive requirement constitutes a threshold minimization obligation: to demonstrate some reasonable belief that the surveillance is in the best interest of the child. A parent is not authorized to wiretap or bug conversations to gather evidence that would later justify the surveillance. For the surveillance to be legal under the vicarious consent doctrine, evidence that would justify the surveillance must be acquired before the surveillance itself.¹⁰⁹

Whether additional self-minimization requirements are imposed under the vicarious consent doctrine is not as clear. Are lawyers or parents required to delete conversations that are clearly not relevant conversations? One problem is with the use of voice activated recording devices. If such a device is placed on a phone or placed in a bug in the room, all of the conversations in the room or over the telephone are recorded. A less inherently pervasive use of technology would be for the eavesdropping parent to only trigger the recording when he or she knows the minor is talking to the other parent on the telephone. This might be unacceptable because it would limit the recording to only when the parent is at home. One might suggest a minimization requirement analogous to the Wiretap Act that would require the recording parent to delete conversations that are not relevant to the best interests of the child. The obvious problem with this requirement is the credibility of the resulting tape in the face that it has been tampered with.

The previous sub-sections have discussed the vicarious consent principal in two regards: (1) they have provided an interpretation of the scope and requirements of the rule and (2) offered a critique of the rule. In view of the problems discussed above, the vicarious consent principle cannot be supported. The vicarious consent doctrine should be junked in those jurisdictions that have adopted it and not recognized by other courts in the future.

109. See generally *Pollock v. Pollock*, 154 F.3d 601 (6th Cir. 1998) (noting that the legitimacy of the surveillance hinges on the consenting parent's objective good faith concern that taping is in the child's best interest).

F. Silent Video Surveillance

Video surveillance without an accompanying audio component (silent video surveillance) is not a violation of The Wiretap Act of the ECPA.¹¹⁰ The acquisition of an image is not an interception of a wire or oral communication because the contents of a conversation are not acquired. Video surveillance is not the interception of an electronic communication under The Wiretap Act of the ECPA because there has been no interception of the image while it is being transmitted. The audio portion of a videotape is an oral communication and would be subject to the rules discussed above for interspousal or parental bugging.¹¹¹ This is also the emerging view in cases arising under state wiretap statutes.¹¹²

G. The Role of State Law

The question of whether it is legal for a spouse to record the conversations of another spouse in the family home under state wiretap statutes is more complicated. First, the Wiretap and Stored Communications Acts adopt a floor preemption rule allowing state wiretap and stored communications acts to provide for greater security for conversational privacy and for access to e-mail and voicemail (stored electronic communications).¹¹³ Therefore, state law may be written or construed to not provide for a marital conflict exception without violating the Federal Wiretap Act. Second, in civil actions brought for violations of the state statute the tort interspousal immunity defense may be available to the wiretapper.

1. Interspousal Exceptions Under State Law

There are only a few state courts that have examined the question of whether the applicable state wiretap statute contains an exception for interspousal wiretapping. Most of the courts that have addressed the question have construed states laws not to contain an interspousal wiretapping exception.¹¹⁴ It should be noted that state courts within

110. This is the view of all of the federal circuits that have considered the question. See, e.g., *United States v. Falls*, 34 F.3d 674, 679-80 (8th Cir. 1994); *United States v. Torres*, 751 F.2d 875, 885-86 (7th Cir. 1984).

111. See *supra* notes 52-93 and accompanying text.

112. See, e.g., *State v. Diaz*, 706 A.2d 264, 268 (N.J. Super. Ct. App. Div. 1998); *Ricks v. State*, 537 A.2d 612, 616 (Md. 1988); *People v. Teicher*, 422 N.E.2d 506, 513 (N.Y. 1981).

113. See, for example, *State v. Ayres*, 383 A.2d 87 (N.H. 1978), where the New Hampshire Supreme Court discussed the stricter consent rule under the state of New Hampshire's wiretap act, chapter 570-A of the New Hampshire Revised Statutes Annotated.

114. See generally Stacy L. Mills, Note, *He Wouldn't Listen to Me Before, But Now . . . : Interspousal Wiretapping and An Analysis of State Wiretapping Statutes*, 37

the two federal circuits that recognize the interspousal wiretapping exception under federal law are not bound by interpretations of federal law in interpreting state wiretap acts, even if the state statute tracks the language of the Wiretap Act. In *Ransom v. Ransom*,¹¹⁵ the Supreme Court of Georgia rejected the intercepting spouse's contention that the state wiretap statute should be construed to recognize an interspousal wiretap exception as the Fifth Circuit had done in *Simpson*.¹¹⁶ In rejecting this contention, the court relied on the state statute's purpose to protect every citizen's privacy and on the fact that the language of the statute did not contain an exception for interspousal wiretapping.¹¹⁷ New York, like Georgia, does not recognize an interspousal exception under the New York Wiretap Act.¹¹⁸

2. *The State Interspousal Tort Immunity Defense*

Interspousal tort immunity could provide a defense to civil suits for violation of state wiretap acts in cases where the state statute was not construed to contain an interspousal exception. In such a case, although the state wiretap statute might have been violated, the general common law defense of interspousal immunity might be a defense to a damage action under the statute.

Courts in states that still recognize interspousal tort immunity have generally not applied the doctrine to actions brought by spouses for violation of the state wiretap act. In *Burgess v. Burgess*,¹¹⁹ the Supreme Court of Florida reversed the lower court and held that the legislature created an exception to the interspousal tort immunity defense in wiretap cases because the result of the defense, admitting the tape into evidence, would be contrary to marital harmony, the often cited purpose of the immunity defense.¹²⁰ The Delaware Superior Court came to the same conclusion in interpreting Delaware law in *State v. Jock*.¹²¹

H. Interspousal and Parental Access to E-Mail: Title I of the ECPA Off the Table

There are only a few appellate court decisions interpreting the legality of interspousal or parental access to e-mail and voicemail. E-

BRANDEIS L.J. 415, 421 (1998) (providing an overarching comparison between state laws and the federal wiretapping statute).

115. 324 S.E.2d 437 (Ga. 1985).

116. *Id.* at 438 (disagreeing with the Fifth Circuit's holding in *Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974)).

117. *Ransom*, 324 S.E.2d at 439.

118. See *Pica v. Pica*, 417 N.Y.S.2d 528 (1979).

119. 447 So. 2d 220 (Fla. 1984).

120. *Id.* at 222-23.

121. 404 A.2d 518 (Del. Super. Ct. 1979).

mail and voicemail cases in other contexts, however, provide a useful basis for evaluation of domestic conflict cases. Access to e-mail and voicemail by private parties is primarily regulated under Title II of the ECPA.¹²² Title II regulates access to "stored electronic communications."¹²³ Communications such as e-mail that consist of purely electronic data are electronic communications. Under the recently enacted USA PATRIOT ACT (Patriot Act) amendments to the ECPA, voicemail is now treated in the same manner as e-mail.¹²⁴

It is well established under federal court precedent that once e-mail is received and stored in a computer system it is regulated exclusively under the Stored Communications Act. Or to put it another way, these cases hold that accessing stored e-mail is not an "interception" of an electronic communication under the Wiretap Act. The amendments of the Patriot Act would apply the same rule to voicemail.

Although the Supreme Court has not decided this question, the decisions of the two federal circuit courts that have considered the issue indicate that once e-mail is stored, it is exclusively regulated by the Stored Communications Act.¹²⁵ In 1994, the Fifth Circuit initially construed the ECPA to restrict interception under the Wiretap Act to the contemporary acquisition of the contents of a conversation or communication in *Steve Jackson Games v. United States Secret Service*.¹²⁶ This construction of the Wiretap Act was initially rejected by the Ninth Circuit in *Konop v. Hawaiian Airlines*¹²⁷ in 2001. The *Konop* court held that e-mail could be intercepted after it was received.¹²⁸ Furthermore, the court held that the accessing and downloading of an e-mail could constitute a violation of both the Wiretap Act and the Stored Communications Act.¹²⁹ In a 2002 re-issue of its previous decision, however, the Ninth Circuit changed its view and concurred with

122. Regulations of government access to e-mail and voicemail, unlike access by a private party, may be subject to constitutional restraints under the Fourth Amendment. See, e.g., *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001); *United States v. Maxwell*, 45 M.J. 406 (1996).

123. See generally 18 U.S.C. §§ 2701-2711 (2000).

124. See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, H.R. 3162, 107th Cong. § 209 (2001) (enacted) [hereinafter the Patriot Act]. For a general analysis of the implications of the Patriot Act voicemail amendment to the ECPA, see *TURKINGTON & ALLEN*, *supra* note 6, at 342-45.

125. See *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 236 F.3d 1035 (9th Cir. 2001), *withdrawn by* 262 F.3d 972 (9th Cir. 2001).

126. 36 F.3d 457 (5th Cir. 1994).

127. 236 F.3d 1035 (9th Cir. 2001), *withdrawn by* 262 F.3d 972 (9th Cir. 2001).

128. *Id.* at 1046.

129. *Id.* at 1051.

the Fifth Circuit's *Jackson Games* view on the scope of the ECPA's protection for e-mail.¹³⁰

The Fifth and Ninth Circuits' narrow construction of the scope of protection of e-mail has been severely criticized in commentary and is by no means a compelling or rational interpretation of the ECPA. Nevertheless, the absence of a contrary federal circuit court construction of the federal statute has resulted in the creation of e-mail policies in the private sector that have relied upon this view of e-mail protection under federal law.¹³¹ In the absence of Supreme Court precedent, which is unlikely, the current view adopted by the Fifth and Ninth Circuits, that e-mail that has been received is exclusively subject to regulation under the Stored Communications Act, is controlling. The net effect of this precedent is that spousal access to stored e-mail is regulated by federal and state stored communications acts.

IV. TITLE II, THE STORED COMMUNICATIONS ACT: DOWNLOADING E-MAIL FROM COMPUTERS LOCATED IN THE HOME

In a case where a spouse or parent accesses e-mail from a computer in the home, the Stored Communications Act may be violated. Section 2701(a) prohibits the intentional accessing and obtaining of e-mail or voicemail (electronic communications) without authorization while it is in electronic storage.¹³²

A. Separate E-Mail Accounts and Separate Passwords

Efforts by spouses to segregate e-mail accounts and maintain separate private passwords are important in evaluating whether access to e-mail stored on the hard drive of a family computer is "without authorization" within the meaning of the Stored Communications Act. Spouses who share access to the hard drive of a mutually used computer located in the homes, but do not share passwords, do not have authority to access the password protected e-mail files of the other spouse. Authorized access to the hard drive does not imply authority to access files that are password protected when the password has been withheld. By maintaining a separate password, the spouse has affirmatively intended to exclude the other spouse from the personal e-mail file. As yet there have been no reported cases under federal or state stored communications acts, but a Fourth Circuit case on analo-

130. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

131. See *TURKINGTON & ALLEN*, *supra* note 6, at 335-39.

132. 18 U.S.C. § 2701 (2000). Section 2701(a) also prohibits the alteration of e-mail or voicemail (electronic communications) and acts that prevent authorized access to e-mail or voicemail. For the e-mail or voicemail to come within § 2701 it must be in a facility through which an electronic communications service is provided. *Id.*

gous facts persuasively rejects the contention of implied authority because of mutual access to the hard drive of a computer in the home.

In *Trulock, III v. Freeh*,¹³³ the court held that authority to generally access the computer hard drive did not include the authority to access password protected files of a joint computer user. Linda Conrad and Notra Trulock jointly used the same computer in an apartment they shared. They protected their personal files with passwords. Conrad consented to government access to Trulock's protected password files. In rejecting the government's contention that Trulock could consent to the Fourth Amendment Search of Conrad's files, the court concluded:

By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. Moreover, because he concealed his password from Conrad, it cannot be said that Trulock assumed the risk that Conrad would permit others to search his files. Thus, Trulock had a reasonable expectation of privacy in the password-protected computer files and Conrad's authority to consent to the search did not extend to them.¹³⁴

B. The "In Electronic Storage" Requirement of Title II

The requirement that the e-mail or voicemail be in electronic storage may eliminate the Stored Communications Act from applicability in many domestic conflict cases where the e-mail is in the hard drive of the computer in the family home. As noted above, only e-mail that is in "electronic storage" is protected from unauthorized access under § 2701 of the Stored Communications Act. Electronic storage is defined in the ECPA as "temporary, immediate storage incidental to the electronic transmission" or "backup" storage of an electronic communication.¹³⁵ In *Fraser v. Nationwide Mutual Insurance Co.*,¹³⁶ Judge Brody took judicial notice of the technology of e-mail transmission that has been invoked favorably by other courts.

Transmission of e-mail from the sender to the recipient through an electronic communication system . . . is indirect. First, an individual authorized to use the system logs on the system to send a message. After a message is sent, the system stores the message in temporary or intermediate storage. I will refer to this storage as "intermediate storage." After a message is sent, the system also stores a copy of the message in a separate storage for back-up protection, in the event that the system crashes before transmission is completed. I will refer to this storage as "back-up protection storage." In the course of trans-

133. 275 F.3d 391 (4th Cir. 2001) (noting that the password-protected computer files were accessed by an FBI computer specialist).

134. *Id.* at 403. Trulock brought a *Bivens* action against former FBI Director Louis Freeh and others for violation of his Fourth Amendment rights. The Fourth Circuit held that Freeh enjoyed qualified immunity for the illegal search because the contours of Fourth Amendment computer consent law had not been established at the time of the illegal search of Trulock's files. *See generally id.*

135. 18 U.S.C. § 2510(17) (2000).

136. 135 F. Supp. 2d 623 (E.D. Pa. 2001).

mission from the sender to the recipient, a message passes through both intermediate and backup protection storage.

Transmission is completed when the recipient, logs on to the system and retrieves the message from intermediate storage. After the message is retrieved by the intended recipient, the message is copied to a third type of storage, which I will call "post-transmission storage." A message may remain in post-transmission storage for several years.¹³⁷

The court in *Fraser* went on to hold that access to e-mail was not subject to the Stored Communications Act regulation because "post-transmission storage" is not "in electronic storage."¹³⁸

C. *White v. White*¹³⁹

The Stored Communications Act prohibits unauthorized access to an electronic communication (e-mail) while it is in "electronic storage."¹⁴⁰ Wiretap statutes in states like New Jersey contain language that tracks the Federal Stored Communications Act.¹⁴¹ In *White v. White*,¹⁴² the court evaluated the applicability of state and federal statutes to interspousal access to e-mail stored on a computer in the family home.¹⁴³ The case illustrates issues that face lawyers in such cases. In *White*, although separated, the husband and wife lived in the same house.¹⁴⁴ The husband occupied the sunroom of the home where the family computer, television, and stereo were located.¹⁴⁵ The sun room was also the only way to get to the grill on the deck of the house.¹⁴⁶ As a result, all of the members of the family were in and out of the room.¹⁴⁷ After the wife discovered a letter from the husband to his girlfriend, allegedly in plain view, she hired a computer detective. The detective, at the wife's direction and without using the husband's password, copied his e-mails that were stored on the hard drive.¹⁴⁸ The court held there was no violation of the New Jersey

137. *Id.* at 633-34 (citations and footnotes omitted).

138. *Id.* at 636 (noting the inapplicability of the Stored Communications Act).

139. 781 A.2d 85 (N.J. Super Ct. Ch. Div. 2001).

140. 18 U.S.C. § 2701(a)(1)-(2) (2000).

141. See N.J. STAT. ANN. § 2A: 156A-27(a) (West Supp. 2003).

142. *White v. White*, 781 A.2d 85 (2001).

143. *Id.* at 86-87.

144. *Id.* at 87.

145. *Id.*

146. *Id.*

147. *Id.* at 92.

148. *Id.* at 87. When installing the America Online (AOL) software, the program automatically created the Personal Filing Cabinet (PFC) on the hard drive of the family computer. The PFC automatically saved e-mail but the e-mail was not automatically password protected and could be accessed by simply opening up the AOL files on the hard drive. The e-mail could have easily been protected by a password or by deletion. The husband, however, did not know the e-mail was saved on the hard drive and took no steps to protect them. *Id.* at 87-88.

Wiretap Act for two reasons.¹⁴⁹ First, the e-mail was not in "electronic storage" when it was accessed.¹⁵⁰ Second, access to the e-mail was not "without authorization" as meant by the Act.¹⁵¹

a. E-Mail Was Not In "Electronic Storage"

In *White*, the court adopted the accepted technical description of transmission of e-mail.¹⁵² E-mail typically involves three stages of storage, intermediate, back-up protection storage, and post-transmission storage.¹⁵³ Once e-mail has been retrieved by the recipient and stored, it is in the post-transmission storage stage.¹⁵⁴ Post-transmission storage was not "electronic storage" within the meaning of the Wiretap Act.¹⁵⁵ The Stored Communications Act protected only electronic communications that are "in the course of transmission or are backup to that course of transmission."¹⁵⁶ This construction of federal and state stored communications acts take wiretap statutes off the table in cases where spouses access e-mail stored on the hard drive of a computer in the family home.

b. Unauthorized Use

In *White*, the court also concluded that access of the e-mail was not "without authorization" as that concept is meant under the Act.¹⁵⁷ "[W]ithout authorization" was limited to prohibited use of a computer or unauthorized use of someone's password.¹⁵⁸ Because the husband in *White* had consented to his wife's access to the computer, her "roaming in and out of different directories on the hard drive" was not "without authorization."¹⁵⁹

D. The Interspousal Exception

New Jersey was one of a majority of states that had construed their state wiretap statute to not contain an exception for interspousal wiretapping. The court in *White* took the same position on the stored electronic communications portion of the Act.¹⁶⁰ Although the court did not have to discuss the question, it held that the New Jersey Wiretap

149. *Id.* at 90-91.

150. *Id.* at 91.

151. *Id.* at 90-91.

152. *Id.* at 89.

153. *Id.* at 89-90.

154. *Id.* at 90.

155. *Id.*

156. *Id.* at 90 (citing *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 637 (E.D. Pa. 2001) (construing the Stored Communications Act)).

157. *Id.* at 90-91.

158. *Id.* at 90.

159. *Id.* at 91.

160. *See id.*

Act did not impliedly exempt interspousal accessing of e-mail in the computer of the home.¹⁶¹

E. The Privacy Intrusion Tort

Most states have recognized a right to privacy tort under state common law. The seminal call for recognition of privacy rights was made in a famous article published in the *Harvard Law Review* in 1890 authored by Samuel D. Warren and Louis D. Brandeis.¹⁶² In the article, the authors focused on tort liability for media publicity of the private lives of public figures. The current formulation of the common law of privacy was greatly influenced by an article written by the late Dean William Prosser in the *California Law Review* in 1960.¹⁶³ In that article, Prosser argued that four torts had emerged from the large body of common law precedent.¹⁶⁴ Prosser argued that although the torts were referred to as involving invasions of privacy, they really involved different kinds of torts and different invasions.¹⁶⁵ The four-part interest analysis and disparate tort theory that Prosser advocated was adopted by the *Restatement (Second) of Torts* in section 652.¹⁶⁶ The *Restatement (Second)* has been influential and is generally embraced by courts as an initial premise in analysis of privacy tort claims.¹⁶⁷ The four torts recognized in the *Restatement (Second)* are: (1) intrusion upon seclusion; (2) appropriation of name or likeness; (3) publicity given to private life; and (4) publicly placing a person in false light.¹⁶⁸ Of these, the privacy intrusion tort is the most relevant to electronic surveillance in domestic disputes. This tort focuses on invasions of informational or physical privacy through the acquisition of personal information about a person or through physical invasions of a person's space or body.

The common law privacy intrusion tort is violated if someone intentionally intrudes upon the private affairs, seclusion, or solitude of another person by means that would be highly offensive to a person of ordinary sensibilities.¹⁶⁹ Recently, the Supreme Court of California

161. See *id.* at 88 (noting the state legislature considered and then rejected interspousal immunity under the New Jersey Wiretap Act).

162. See Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

163. See William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

164. *Id.*

165. *Id.*

166. See RESTATEMENT (SECOND) OF TORTS § 652 (1977).

167. See Jay M. Feinman, *Doctrinal Classification and Economic Negligence*, 33 SAN DIEGO L. REV. 137, 141 (1996) (noting widespread adoption of the RESTATEMENT (SECOND) OF TORTS).

168. See RESTATEMENT (SECOND) OF TORTS §§ 652B-652E (1977).

169. RESTATEMENT (SECOND) OF TORTS § 652B (1977). Most states have adopted the RESTATEMENT (SECOND) OF TORTS version of the privacy intrusion tort.

has articulated an important formulation of the intrusion element of the tort.¹⁷⁰ The intrusion element is established if the plaintiff demonstrates that the defendant has "penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff . . . if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source."¹⁷¹ Core examples of privacy intrusions provided by the *Restatement (Second)* include: (1) forced entry into a hotel room or home; (2) looking into someone's bedroom with binoculars; (3) opening private personal mail; (4) searching a safe, wallet, or private bank account; and (5) tapping telephone lines.¹⁷²

It is well established that an invasion of privacy claim, based on an intrusion theory, does not require that information or images that are the object of the intrusion be published or used in any way. The tort is established by the acquisition of information or the invasion of someone's physical space.¹⁷³ A leading case illustrating this last point is *Hamberger v. Eastman*.¹⁷⁴ The New Hampshire Supreme Court found a privacy intrusion violation when the defendant surreptitiously placed an audio tape recorder in the plaintiffs' bedroom.¹⁷⁵ The court found the conduct actionable even though there was no allegation that anyone had listened to the tape:

If the peeping Tom, the big ear and the electronic eavesdropper (whether ingenious or ingenuous) have a place in the hierarchy of social values, it ought not to be at the expense of a married couple minding their own business in the seclusion of their bedroom who have never asked for or by their conduct deserved a potential projection of their private conversations and actions to their landlord or to others. Whether actual or potential such "publicity with respect to private matters of purely personal concern is an injury to personality. It impairs the mental peace and comfort of the individual and may produce suffering more acute than that produced by a mere bodily injury."¹⁷⁶

The view that the intrusion itself is a sufficient affront to personal dignity to be actionable is also reflected in the damage requirement for privacy intrusion tort actions. Credible evidence of emotional distress is sufficient in privacy tort actions.¹⁷⁷ Expert testimony is not re-

170. See *Shulman v. Group W Productions, Inc.*, 955 P.2d 469 (Cal. 1998).

171. *Id.* at 490 (noting the requirements for a cause of action for intrusion).

172. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

173. *Id.*

174. 206 A.2d 239 (N.H. 1964).

175. *Id.* at 242 (holding defendant liable for privacy intrusion).

176. *Id.* (quoting III POUND, JURISPRUDENCE 58 (1959)).

177. See *Monroe v. Darr*, 559 P.2d 322, 327 (Kan. 1977) (noting that scant amount of evidence of the plaintiffs' mental distress was enough to send question to jury); *Trevino v. Southwestern Bell Tel. Co.*, 582 S.W.2d 582, 584 (Tex. App. 1979) (noting that, because of the nature of the tort at issue, physical damages are unnecessary); DAVID. A. ELDER, THE LAW OF PRIVACY, § 2:10, at 57-61 (1991).

quired for the issue of damages to go to the jury.¹⁷⁸ Section 652H of the *Restatement (Second)* supports this view:

One who has established a cause of action for invasion of his privacy is entitled to recover damages for

- (a) the harm to his interest in privacy resulting from the invasion;
- (b) his mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and
- (c) special damage of which the invasion is a legal cause.¹⁷⁹

Some defendants have argued that the privacy intrusion tort ought to require a showing of extreme or heightened emotional distress analogous to that required in an intentional infliction of emotional distress (IIED) case. The best interpretation of the *Restatement (Second)* and the above authority is that the privacy intrusion tort does not require such a showing of extreme or heightened emotional distress and differs from the IIED in two other important respects.¹⁸⁰ First, the IIED requires a threshold demonstration of conduct by the defendant that is extreme and outrageous in the sense that the conduct is beyond that which is tolerated in a civilized society.¹⁸¹ In a privacy intrusion tort action, the intrusion must be substantial in the sense that the means are highly offensive to an ordinary person. The privacy invading conduct must violate community standards of decency in an intrusion action, but it need not reach the level of social condemnation that is required for IIED. Second, and most importantly, the quantum of evidence of emotional distress that is required for the case to go to the jury is much less in an intrusion action. Credible evidence of emotional distress resulting from the intrusion is sufficient for the jury to consider compensatory damages in an intrusion action. This may be demonstrated without expert testimony.¹⁸² The threshold quantum of evidence in an IIED action is greater and requires demonstration of a "severe and disabling emotional or mental condition" generally recognized by trained professionals.¹⁸³

The interrelationship between the wiretap acts and the common law privacy intrusion tort in family and custodial dispute electronic surveillance cases is illustrated by a recent Supreme Court of New Hampshire case. In *Fischer v. Hooper*,¹⁸⁴ a divorced husband taped the conversations of his former wife and daughter without obtaining

178. See *Fischer v. Hooper*, 732 A.2d 396, 402 (N.H. 1999) (citing *Monroe v. Darr*, 559 P.2d 322, 327 (Kan. 1977)).

179. RESTATEMENT (SECOND) OF TORTS § 652H (1977).

180. See *Miller v. Brooks*, 472 S.E.2d 350 (N.C. Ct. App. 1996) (distinguishing elements required for cause of action under tort of outrage and privacy intrusion tort).

181. RESTATEMENT (SECOND) OF TORTS § 46 cmt. d (1965).

182. See *Fischer*, 732 A.2d at 401 (noting that expert testimony was not required).

183. *Waddle v. Sparks*, 414 S.E.2d 22, 27 (N.C. 1992) (quoting *Johnson v. Ruark Obstetrics & Gynecology Ass'n*, 395 S.E.2d 85, 97 (N.C. 1990)).

184. 732 A.2d 396 (N.H. 1999).

either party's consent.¹⁸⁵ Upon discovering this, the wife brought a cause of action under the state wiretap act and for invasion of privacy under the state common law.¹⁸⁶ The court remanded the case for further findings of fact on the state wiretap count, but affirmed the lower court's decision that the plaintiff's privacy intrusion tort action was properly submitted to the jury.¹⁸⁷

In *Fischer*, the parties had joint custody of their daughter, and a guardian ad litem and a therapist had been appointed for their daughter.¹⁸⁸ The husband argued that the wife had no reasonable expectation of privacy of her conversations with her daughter because she should have expected that the daughter would divulge the content of their conversations to the therapist.¹⁸⁹ Even if this were the case, the court concluded that the jury might have concluded that the plaintiff had a reasonable expectation of privacy that her actual voice and words would not be "captured on tape."¹⁹⁰

Fischer assumes as a basis of its intrusion tort holding that wiretap legislation and common law privacy tort claims exist as separate legal claims even though the misconduct that is the basis of the wiretap and privacy intrusion tort actions is the same. In the absence of a clear intention that the wiretap act was intended to preempt the state common law, electronic surveillance that constitutes an intrusion should be actionable even though it might also be a violation of wiretap legislation. Given this view that state wiretap and privacy intrusion tort claims exist as separate claims, conduct that did not violate the wiretap act might constitute a violation of the privacy intrusion tort. This is the view of the Supreme Court of California.¹⁹¹

a. Invasions of Privacy and Intentional Infliction of Emotional Distress

As noted above, privacy intrusion and IIED actions do not track each other. In some marital conflict cases, however, electronic surveillance can be sufficiently outrageous to constitute both torts. A North Carolina appeals court, in *Miller v. Brooks*,¹⁹² found this to be the

185. *Id.* at 398.

186. *Id.*

187. *Id.* at 398, 402 (noting the holding of the court with respect to privacy and state wiretap claims).

188. *Id.* at 398 (noting the status of custody).

189. *Id.* at 400 (noting the contentions of the defendant regarding plaintiff's alleged diminished expectation of privacy).

190. *Id.* at 401 (stating the court's rationale).

191. See *Shulman v. Group W Productions, Inc.*, 955 P.2d 469 (Cal. 1998) (holding that recordings of conversations at the scene of an automobile accident did not violate the California Wiretap Act, but did constitute privacy intrusion tort under state law).

192. 472 S.E.2d 350 (N.C. Ct. App. 1996).

case. In *Miller*, the wife, Annette Miller, hired a private detective to install a hidden video camera in the bedroom ceiling of the home after she was separated and agreed not to return to her former marital home.¹⁹³ She also represented herself as a resident of the home and intercepted some of her estranged husband's mail.¹⁹⁴ Terry Miller, the husband, sued his estranged wife and the detectives she had hired for privacy intrusion, IIED, and trespass to real property.¹⁹⁵ The trial court granted summary judgment to the defendants in respect to all of plaintiff's claims.¹⁹⁶ The court of appeals reversed, holding that the plaintiff had presented evidence that was sufficient to go to a jury on all claims.¹⁹⁷

Defendants contended that the husband had a reduced expectation of privacy because of his marriage to defendant Annette Miller.¹⁹⁸ In rejecting this argument the court noted:

Although a person's reasonable expectation of privacy might, in some cases, be less for married persons than for single persons, such is not the case here where the spouses were estranged and living separately. Further, the marital relationship has no bearing on the acts of [the private detectives]. Plaintiff's marriage to defendant Miller did nothing to reduce his expectations that his personal privacy would not be invaded by perfect strangers.¹⁹⁹

The video surveillance, opening of the mail, and trespass into the plaintiff's property also constituted sufficiently extreme and outrageous conduct for the jury to consider emotional distress damages for IIED.²⁰⁰ The court also ruled that the plaintiff had established sufficient evidence of aggravated conduct for the jury to award punitive damages for both the privacy intrusion and IIED torts.²⁰¹

b. Privacy Intrusion Tort and Silent Video Surveillance

In cases where federal or state wiretap and stored communications acts are not violated, the common law privacy intrusion tort may apply to wiretapping, bugging, silent video surveillance, or electronic downloading of e-mail that are employed in domestic or custodial conflicts. As noted in section F above, silent video surveillance is not regulated under state and federal wiretap acts. The common law privacy intrusion tort may apply to silent video surveillance and other forms of electronic surveillance that are employed in domestic or custodial conflicts that do not violate federal or state wiretap and stored elec-

193. *Id.* at 352 (noting the actions of defendants).

194. *Id.* at 353 (noting the actions of defendant).

195. *Id.*

196. *Id.*

197. *Id.* at 357 (stating the disposition of case).

198. *Id.* at 354-55 (noting the contention of defendants).

199. *Id.* at 355.

200. *Id.* at 356 (noting the sufficiency of evidence for submission to jury).

201. *Id.* at 357 (reversing summary judgment on the issue of damages).

tronic communications acts. Nonetheless, as discussed below, while the intrusion tort would provide a complimentary compensatory damage remedy, the invasion of privacy would not be a basis for excluding the fruits of the tortuous conduct in divorce or custody proceedings.²⁰²

A privacy intrusion tort action might be available in silent video recordings cases if the video captured images of someone in a private place where he or she had a reasonable expectation of privacy.²⁰³ As illustrated by the court in *White v. White*,²⁰⁴ the privacy intrusion tort gives courts flexibility through the "reasonable expectation of privacy" and "highly offensive means" elements.²⁰⁵ This renders the particular circumstances of the wiretapping, bugging, or silent video surveillance critical to the court's analysis. For example, in *Alexander v. Pathfinder, Inc.*,²⁰⁶ the court held that the audio taping of conversations between a mother and staff in a facility for the mentally retarded was not an intrusion upon the seclusion of the mother because she knew the conversations were being recorded and did not object.²⁰⁷ Moreover, in *Deteresa v. ABC*,²⁰⁸ the surreptitious audio and videotaping by a television producer of a woman who would not appear on his show was found not to be a violation of the privacy intrusion tort because the videotaping occurred in a public place.²⁰⁹ The audio taping was not sufficiently offensive to be actionable because she had spoken to a person she knew was a reporter.²¹⁰ Compare these decisions with the California Supreme Court's view in *Sanders v. ABC*.²¹¹ In *Sanders*, the court held that a telepsychic had a reasonable expectation of privacy in conversations with an agent of ABC held in a large room with rows of cubicles (about 100) in which psychics took their calls.²¹²

There is general legal recognition that a person has a reasonable expectation of privacy in their conversations or conduct at their

202. See *infra* section III.D.

203. See *McCray v. State*, 581 A.2d 45, 48 (Md. Ct. Spec. App. 1990) (holding that government video taping was not a search because a person walking on a public sidewalk or street has no reasonable expectation of privacy in activities in public view).

204. 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001).

205. See *generally id.* (holding that a wife's intrusion into her husband's e-mail that was stored on the hard drive of the family computer was not "highly offensive" given that the husband had no "reasonable expectation of privacy" in the area).

206. 189 F.3d 735 (8th Cir. 1999).

207. See *id.* at 742-43 (noting fact that mother did not object to recording by institution's employees).

208. 121 F.3d 460 (9th Cir. 1997).

209. *Id.* at 466 (refusing to sustain cause of action where plaintiff was videotaped in public view).

210. *Id.* (noting that the plaintiff knew the person was a reporter).

211. 978 P.2d 67 (Cal. 1999).

212. *Id.* at 923

home.²¹³ Surreptitious wiretapping, bugging, or video surveillance in a person's home clearly constitutes an intentional intrusion into the subject's seclusion or private affairs. Courts early on recognized surreptitious audio taping by a landlord in a tenant's bedroom as an invasion of privacy.²¹⁴ Moreover, the *Restatement (Second)* considers surreptitious video and audio surveillance to be a paradigm of intrusion into seclusion and private affairs.²¹⁵

Surreptitious wiretapping, bugging, and videotaping in domestic and custodial conflicts have generally been found to be actionable intrusions. Courts that have considered wiretap act construction have not been inclined to recognize a marital conflict or vicarious consent defense in privacy intrusion tort actions. The notion of vicarious consent is irrelevant in a privacy intrusion tort action. Consent is a defense to the tort action, but it is the consent of the party whose privacy is invaded that is relevant. Even if the custodial parent could consent for the child, there could be no vicarious consent to the invasion of privacy of the non-custodial parent or other third parties. There, consent would be governed by general tort principles of actual, express, or implied consent.²¹⁶

For example, in *Fischer*, the New Hampshire Supreme Court found that a custodial parent's taping of telephone conversations between his daughter and former wife to have constituted an intrusion.²¹⁷ Although the court had appointed a therapist for the daughter, the court found that the mother retained a reasonable expectation that the conversation would not be electronically recorded because the mother should have expected that the daughter would discuss her conversations with the therapist.²¹⁸ The court treated consent to be governed by general tort principles.²¹⁹ Similarly, the North Carolina Court of Appeals found that the placement of a hidden video camera in the

213. See *Kyllo v. United States*, 533 U.S. 27 (2001); *Katz v. United States*, 389 U.S. 347 (1967).

214. See *Hamberger v. Eastman*, 206 A.2d 239 (N.H. 1964).

215. See *RESTATEMENT (SECOND) OF TORTS* § 652B cmt. b (1977).

216. See *Dieteman v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971) (holding no express or implied consent for surreptitious photography and audio taping of office visit when Dieteman invited reporter claiming to be patient into office in Dieteman's home); *RESTATEMENT (SECOND) OF TORTS* § 652 (1977).

217. *Fischer v. Hooper*, 732 A.2d 396, 398-401 (N.H. 1999).

218. *Id.*

219. See *id.* at 405. The court held that the trial court had properly instructed the jury that whether the mother had impliedly consented to the surveillance, depended upon whether her conduct in fact constituted implied consent and that the trial court did not error in failing to include the term "acquiescence" in the instructions to the jury on consent. *Id.*

home and bedroom of an estranged husband by his wife was a highly offensive intrusion into his private affairs and seclusion.²²⁰

c. Interspousal Access to E-Mail and the Privacy Intrusion Tort

Employees seeking damages for violation of the privacy intrusion tort against employers who accessed their e-mail have generally been unsuccessful. Courts have used the alternative grounds that the employee has no reasonable expectation of privacy in e-mail stored in a business computer network and that employer access is not an offensive means within the privacy intrusion tort. This has been the holding even if the employer published policy was that e-mail communications are confidential and not monitored. A leading and controversial case is *Smyth v. Pillsbury Co.*²²¹ There, a federal district court held Smyth had no reasonable expectation of privacy in e-mail communications to a supervisor over an e-mail system that was "apparently utilized by the entire company."²²² The court also found accessing the particular communications was not a "highly offensive invasion of privacy."²²³ A Texas court of appeals court took a similar view in *McClaren v. Microsoft Corp.*²²⁴ A superior court in Massachusetts, however, has taken a different view and would recognize a reasonable expectation of privacy in employee e-mail.²²⁵

The validity of decisions that fail to recognize that employees have reasonable expectations of privacy in privacy intrusion tort actions brought against employers for access to employee e-mail in company e-mail systems is beyond the scope of this Article. It is clear, however, that these cases do not control the question of whether spousal access to e-mail stored in a computer in the family or marital home is a violation of the privacy intrusion tort. As proprietors of company e-mail systems, employers have authority to access employee e-mail under the Stored Communications Act.²²⁶ Even employees have reasonable

220. See *Miller v. Brooks*, 472 S.E.2d 350, 354 (N.C. Ct. App. 1996). The defendant wife's conduct also included opening the husband's mail. *Id.* The case, however seems to hold that the video surveillance by itself was sufficient to constitute a privacy intrusion cause of action.

221. 914 F. Supp. 97 (E.D. Pa. 1996).

222. *Id.* at 101 (holding Smyth did not have a reasonable expectation of privacy).

223. *Id.* (holding that access to Smyth's e-mails was not "highly offensive").

224. No. 05-97-00824-CV, 1999 WL 339015, at *4-*5 (Tex. App. May 28, 1999) (not designated for publication) (holding that access to an employee e-mail by another employee was not highly offensive and the employee did not have a reasonable expectation of privacy).

225. See *Restuccia v. Burk Tech., Inc.*, No. CA 952125, 1996 WL 1329386, at *3 (Mass. Super. Aug. 13, 1996).

226. Section 2701(c) of the Stored Communications Act provides that it is not unlawful to access stored electronic communications if access is authorized "by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1) (2000).

expectations of privacy in e-mail stored outside of company e-mail systems. In a leading case, *United States v. Maxwell*,²²⁷ the court held that a United States Air Force Colonel had a reasonable expectation of privacy in e-mail messages stored in his internet service provider's central computer under a contractual privacy policy not to disclose the e-mail to anyone other than an authorized user or pursuant to a court order.²²⁸

The reasonableness of privacy expectations in e-mail stored in computers in the home will depend upon whether the spouse has consented or authorized access to the e-mail by the other spouse. If separate e-mail accounts and separate passwords are maintained by spouses who jointly share a computer with joint access to the main drive, each spouse would have a reasonable expectation of privacy in their separate e-mail accounts. As observed by the *Trulock* court in the discussion above,²²⁹ a spouse's affirmative act of maintaining a separate e-mail account and password demonstrates an intention to exclude others, including the other spouse, from the personal e-mail files. By this act, the spouse has a reasonable expectation of privacy in the password-protected files.²³⁰

White v. White,²³¹ discussed above, illustrates the importance of password-protected e-mail files in privacy intrusion tort actions. The court in *White* rejected Mr. White's claim that accessing stored e-mail by Mrs. White constituted a violation of the privacy intrusion tort. As correctly observed by the court, the plaintiff must have a reasonable expectation of privacy in the area or information that is accessed and the means of access must be *highly offensive* for a tortious invasion of privacy to occur.²³² Both spouses and their children had authority to access the hard drive of the computer which was located in the sun room of the home. Under the e-mail service agreement with America Online (AOL), and unknown to Mr. White, he was saving e-mail he sent and received on the hard drive of the computer. Because he did not know he was doing this, he did not delete or protect the e-mail with a password. In light of the authority given to both spouses to access the hard drive, Mr. White had no reasonable expectation of privacy in e-mail on the hard drive of the computer. The court analogized the computer to an office file cabinet in a room both spouses had com-

227. 45 M.J. 406 (C.A.A.F. 1996).

228. *Id.* at 417-19 (holding that the Colonel had an expectation of privacy). The e-mail in question was generated by computer hardware, software, and accessories that were purchased and maintained by Maxwell. Use of the computer and services by Maxwell was not in connection with his official Air Force duties. *Id.* at 411.

229. See *supra* note 133 and accompanying text.

230. See *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001); see also *supra* text accompanying notes 125-130.

231. 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001); see also *supra* subsection II.I.3.

232. *Id.* at 91-92.

plete access to.²³³ The privacy intrusion tort becomes important in spousal access to e-mail cases because, as discussed in the section above, several courts have construed the Stored Communications Act as not applying to e-mail stored in computers in the home.²³⁴ As noted in the section below, however, violations of the privacy intrusion tort will provide a damage remedy for the spouse whose privacy is invaded, but the tort violation is not an independent basis for excluding the illegally acquired e-mail from divorce or custody proceedings.²³⁵

V. EXCLUSION OF FRUITS OF ILLEGAL SURVEILLANCE

A. The Fault Requirement for Violation of the ECPA

Criminal responsibility, damage remedies, and the exclusionary rule are only triggered if there is a willful or intentional violation of the ECPA. Section 2511 of the 1968 Wiretap Act limited criminal sanctions to "willful" violations of the statute.²³⁶ Although initially there was no reference to "willful" in § 2520, the damage section of the statute, courts generally required a finding that the defendant had acted willfully for damages to be recoverable.²³⁷ "Willful," within the meaning of § 2511 or § 2520, was interpreted the way it is generally constructed in federal criminal statutes and was not limited to a knowing violation of the statute; "willful" has the broader meaning of "reckless disregard of a known legal duty."²³⁸ As elaborated by a leading case:

The word [willful] often denotes an act which is intentional or knowing or voluntary, as distinguished from accidental. But when used in a criminal statute it generally means an act done with a bad purpose; without justifiable excuse; stubbornly, obstinately, perversely. The word is also employed to characterize a thing done without ground for believing it is lawful, or conduct marked by careless disregard whether or not one has the right so to act.²³⁹

Thus, accidental or negligent violations of the statute will not satisfy the fault requirement in § 2511 and § 2520 of the ECPA. It is enough, however, that the interception was done "without justifiable excuse[,] stubbornly, obstinately, perversely", or "without ground for

233. *Id.* at 92. The analogy was based upon a New Jersey case where the husband unsuccessfully tried to suppress love letters that had been discovered by the wife in file cabinets she had full access to. See *DelPresto v. DelPresto*, 235 A.2d 240, 245-46 (N.J. Super. Ct. App. Div. 1967).

234. See discussion *supra* Part II.I.2. of *White* and other courts not viewing e-mail stored in computers in the home or workplace as "in electronic storage" under state and federal Stored Communications Acts.

235. See *infra* notes 271-75 and accompanying text.

236. See 18 U.S.C. § 2511(1) (2000).

237. See *Citron v. Citron*, 722 F.2d 14, 16 (2d Cir. 1983); *Kratz v. Kratz*, 477 F. Supp. 463, 467 (E.D. Pa. 1979).

238. *Citron*, 722 F.2d at 16.

239. *United States v. Murdock*, 290 U.S. 389, 394-95 (1933) (citations omitted).

believing it was lawful", or with "careless disregard whether or not one [had] the right . . . to act."²⁴⁰

In many cases, "willfully" may be treated as a factual question for the jury. Illustrative of this point is the court's decision in *Citron v. Citron*.²⁴¹ In *Citron*, Fiona Citron taped conversations between her husband and their adopted children, Steven and Alisande.²⁴² She continued to tape the conversations after consulting her attorney.²⁴³ After discovering that some of his conversations with the children had been recorded, Casper, Steven, and Alisande brought a damage action under § 2520 of the Federal Wiretap Act.²⁴⁴ The Second Circuit Court of Appeals affirmed the dismissal of the complaint after the jury in a special verdict found that Fiona had not acted intentionally or recklessly in taping the conversations.²⁴⁵

Citron also reflects the general view taken by courts that § 2511, the "willfulness" standard in the criminal law provision, has the same meanings as in § 2520, the damage section.²⁴⁶ The damage provision of the Wiretap Act provides that a "good faith reliance on . . . a legislative authorization . . . or a statutory authorization" constitutes a defense.²⁴⁷ This section tracks the general notion of "willfulness" required for negligence, but is generally regarded as specifically addressing "good faith" on the part of law enforcement officials or their assistants.²⁴⁸ State courts have construed "willfully" under state wiretap acts similarly.²⁴⁹ Although there is ambiguity in the fault requirement because recklessness is sufficient, it is clear that a jury determination that the defendant acted with a good faith belief that her conduct was lawful is sufficient to satisfy the recklessness requirement.²⁵⁰

The ECPA substituted "intentional" for "willfully" in § 2511 and added "intentional" to portions of § 2520.²⁵¹ Courts generally do not

240. *Citron*, 722 F.2d at 16 (quoting *Murdock*, 290 U.S. at 394-95); see also *Kratz*, 477 F. Supp. at 478-79; *Heggy v. Heggy*, 944 F.2d 1537, 1542 (10th Cir. 1991).

241. 722 F.2d 14 (1983).

242. *Id.* at 15.

243. *Id.*

244. *Id.*

245. *Id.* at 17.

246. *Id.* at 16.

247. 18 U.S.C. § 2520(d)(1) (2000).

248. See *Citron v. Citron*, 722 F.2d 14, 16 (2d Cir. 1983).

249. See *Fischer v. Hooper*, 732 A.2d 396, 400 (N.H. 1999).

250. See *id.*

251. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 101(f), 103, 100 Stat. 1853, 1854 (1986) (codified as amended at 18 U.S.C. §§ 2511, 2520 (2000)).

consider this change to alter the pre-ECPA view that recklessness, as explained above, satisfies the fault requirement.²⁵²

B. The Federal Wiretap's Strict Exclusionary Rule

The Wiretap Act has a strict exclusionary rule.²⁵³ Section 2515 excludes any part of the contents of an illegally intercepted communication from being admitted into any legal proceedings before state or federal legislatures, courts, or administrative agencies.²⁵⁴ Evidence is only excluded under the Wiretap Act if it is the fruit of activities that constitute a violation of the Wiretap Act. Therefore, the fruits of electronic surveillance would be admissible in a state court divorce or custody proceeding if surveillance was exempt from the Wiretap Act because of the spousal marital conflict exception.²⁵⁵ This would also be the case if the electronic surveillance was exempt because the parent had authority to vicariously consent for the child whose conversations were recorded.²⁵⁶ Evidence procured from an interception that was not willful or intentional could also be admitted in state court proceedings as those interceptions are not illegal under the Wiretap Act.²⁵⁷

The exclusionary force of the Wiretap Act violations in state divorce or custody proceedings has been acknowledged by state courts.²⁵⁸ In *In re Marriage of Lopp*,²⁵⁹ the Supreme Court of Indiana held that it was not reversible error for a trial judge to hear wiretaps procured in violation of The Wiretap Act where the wiretap victim claimed that the wiretaps were used by her spouse to blackmail her into signing a provisional custody order.²⁶⁰ The court decided that even if § 2515 generally required exclusion of wiretaps introduced to establish the merits of the controversy, the exclusionary rule was not applicable to conversations introduced to challenge the credibility of witnesses or to conversations that were pertinent to allegations of tes-

252. See *Heggy v. Heggy*, 944 F.2d 1537 (10th Cir. 1991); *Citron v. Citron*, 722 F.2d 14 (2d Cir. 1983), *cert. denied*, 466 U.S. 973 (1984); *Kratz v. Kratz*, 477 F. Supp. 463 E.D. Pa. 1979).

253. See 18 U.S.C. § 2515 (2000).

254. *Id.*

255. As noted earlier the Fifth Circuit and Second Circuit have recognized a limited marital conflict exception. See *supra* notes 58-60 and accompanying text.

256. See *supra* subsection II.E.2.

257. See *supra* section III.A.

258. See *Markham v. Markham*, 265 So. 2d 59, 60 (Fla. Dist. Ct. App. 1972), *aff'd*, 272 So. 2d 813 (Fla. 1973); *Rickenbaker v. Rickenbaker*, 222 S.E.2d 463, 465 (N.C. Ct. App. 1976), *modified*, 226 S.E.2d 347 (N.C. 1976).

259. 378 N.E.2d 414 (Ind. 1978).

260. See *id.* at 422 (noting that the circumstances rendered the court's review of tapes obtained not reversible error).

timony defrauding the court.²⁶¹ To apply the exclusionary rule of § 2515 to such cases would violate the Due Process Clause and constitute an unconstitutional impairment of essential functions of state judges and state sovereignty.²⁶²

Lopp does not represent an important exception to the Wiretap Act's exclusionary rule. The state sovereignty case relied upon in *Lopp* was *National League of Cities v. Usery*.²⁶³ *National League of Cities* held that Federal Commerce Clause legislation imposing a minimum wage requirement on local government entities violated state sovereignty.²⁶⁴ The minimum wage holding of *National League of Cities* was overruled in *Garcia v. San Antonio Metropolitan Transit Authority*.²⁶⁵ Nevertheless, in two cases subsequent to *Garcia*, the Supreme Court has found federal legislation enacted under the Commerce Clause to violate state sovereignty.²⁶⁶ These cases, however, did not involve state activity closely akin to that in *Lopp*. Instead, the cases involved federal legislation that required states to legislate²⁶⁷ and imposed an obligation on state and local law enforcement officers to do background checks and perform other tasks that were connected to the purchase of handguns.²⁶⁸ In *Testa v. Katt*,²⁶⁹ a case more closely related to the state activity in *Lopp*, the Court held that federal legislation requiring state courts to enforce federally created causes of action does not violate state sovereignty. Therefore, because *Lopp* is inconsistent with *Testa*, *Lopp* should not be followed.

C. No Exclusionary Rule Under Title II

As noted earlier, there is no exclusionary rule explicitly in the Stored Communications Act. There is no basis for implying an exclusionary rule because § 2708 specifically states that the remedies under the Stored Communications Act are limited to those that are enumerated.²⁷⁰ As a consequence, even if access to e-mail or voicemail violates the Stored Communications Act, the e-mail or

261. *Id.* (noting that it would be illogical to apply the exclusionary rule under certain circumstances).

262. *See id.* at 423 (noting potential issues of federalism).

263. *See id.* (citing *Nat'l League of Cities v. Usery*, 426 U.S. 833 (1976)).

264. *See Nat'l League of Cities v. Usery*, 426 U.S. 833, 851-52 (1976) (striking down mandatory minimum wage for state employees), *overruled by Garcia v. San Antonio Metro. Transit Auth.*, 469 U.S. 528 (1985).

265. 469 U.S. 528, 531 (1985).

266. *See Printz v. United States*, 521 U.S. 898, 932-33 (1997); *New York v. United States*, 505 U.S. 144, 188 (1992).

267. *New York*, 504 U.S. at 188.

268. *Printz*, 521 U.S. at 932-33.

269. 330 U.S. 386, 393 (1947).

270. *See* 18 U.S.C. § 2708 (2000).

voicemail would be admissible in divorce or custody proceedings in state court.

D. Exclusion of Evidence for Privacy Intrusion Tort Invasions

The absence of an exclusionary rule under the Stored Communications Act means evidence from the fruits of invasions of privacy through illegal access to e-mail and voicemail is admissible in divorce and custody proceedings under the Federal Stored Communications Act. As suggested above, conduct that violates the Stored Communications Act also may constitute an invasion of privacy under common law tort. To determine admissibility, however, it must first be determined whether the common law of torts provides an independent basis for excluding evidence. As a general matter there is no common law exclusionary rule. The fact that evidence is acquired in the commission of a tort is not by itself a sufficient reason for excluding the evidence if it is relevant or material in a subsequent civil or criminal court proceeding. In cases where the government violates constitutional provisions such as the Fourth Amendment, a rule excluding introduction of the fruits of the illegal search has been adopted by the Court as a deterrent to police and on the basis that the government as guardian of our rights should not benefit from acting illegally.²⁷¹ In some instances, such as the Wiretap Act, the legislature has adopted an exclusionary rule to enforce standards in statutes. These exclusionary rules express the idea that privacy, over the integrity of fact finding and the justice dispensing function of courts, should be given priority when enforcing the prohibited statutory conduct. In the case of constitutional or legislative exclusionary rules, exclusion of evidence is designed as a means for enforcing the constitutional or legislative standards and policies that are in place.

Remedies that are built into the remedies that are part of our long-standing common law tort traditions are viewed by courts as sufficient to further tort policies of compensating tort victims and deterring of tortious conduct. Compensatory tort damages include money for physical and emotional pain and suffering as well as out of pocket economic loss. Deterrence is promoted indirectly by granting compensatory damages awards through insurance rates.²⁷² Direct deterrence is promoted through punitive damage awards.²⁷³ Given this, it is not surprising that there is little or no authority to exclude relevant and material evidence in custody or divorce proceedings on the basis that

271. See WAYNE R. LAFAYE ET AL., CRIMINAL PROCEDURE § 3.1 (3d ed. 2000).

272. For a general discussion of the role of compensatory and punitive damages and insurance with regard to deterrence in tort law, see GEORGE C. CHRISTIE ET AL., CASES AND MATERIALS ON THE LAW OF TORTS 735 (3d ed. 1997).

273. See *id.* at 792.

the evidence is the fruit of conduct that constitutes a common law tort violation. There may be cases where a court might exclude evidence in a civil proceeding on the basis of improper conduct of parties or lawyers in those proceedings. In *Shoney's v. Lewis, Inc.*,²⁷⁴ for example, the Kentucky Supreme Court excluded the introduction of evidence that was procured by one of the lawyers before the court in violation of a code of professional conduct rule.²⁷⁵ In that case, however, the court was exercising its authority to sanction conduct that was unethical by a lawyer who is an officer of the court system.

VI. MINIMIZATION OF PRIVACY INVASIONS BY PROTECTIVE ORDERS IN DISCOVERY

As suggested in Parts III and IV of this article, the Wiretap Act and the Stored Communications Act have been construed to allow for the electronic surveillance of communications or conversations without a filtering mechanism that would minimize invasions of privacy of innocent persons; those persons communicating or conversing about matters unrelated to the legitimate justification for the electronic surveillance. The absence of a filtering mechanism for minimization is a serious problem because significant invasions of privacy occur and are sanctioned by law even though there is no justification for the privacy invasions. The minimization problems arises in two related situations: (1) where the ECPA allows for the electronic surveillance of conversations or the unauthorized access to digital communications of innocent persons and (2) where the content of the conversation or communication may be admitted in a judicial proceeding because of the absence of an exclusionary rule.

This section will examine the extent to which privacy protection in discovery rules and under state and federal constitutions may be utilized to function as *de facto* exclusionary rules that minimize the introduction of innocent person's conversations or communications into records of judicial proceedings. Preventing the introduction of innocent personal conversations or communications into court records is important for privacy protection because judicial records are probably the most public records in our legal system.

The ECPA does not provide for exclusion of an innocent person's conversations or communications in two instances. There is no exclusion under The Wiretap Act in cases where courts recognize an exception to unauthorized interceptions of conversations in marital conflicts or for parents intercepting the conversations of their minor children. Although The Wiretap Act has a strong exclusionary rule it does not

274. 875 S.W.2d 514 (Ky. 1994).

275. The attorney violated a rule prohibiting *ex parte* communication between a lawyer and a party represented by another lawyer. See *id.* at 516.

apply because there has been no violation of the Wiretap Act. Perhaps more importantly there is no exclusion under the Stored Communications Act in any case where e-mail or voicemail is accessed even if the access violates the Stored Communications Act. Nevertheless, privacy rights recognized in discovery rules and federal and state constitutions provide rules for preventing innocent persons' communications or conversations from introduction into judicial proceedings.

A. Constitutionally Based Privacy Rights

There are two traditions of privacy rights under the United States Constitution²⁷⁶ and the constitutions of several states. Decisional privacy rights protect independence of decisions for matters such as abortion. Informational privacy rights recognize a right of persons to decide whether the government shall have access to highly personal or intimate information about them. Informational privacy rights are protected under unreasonable search and seizure provisions in the federal and state constitutions. These rights are also protected under the due process clauses of state and federal constitutions.²⁷⁷ Compelled disclosure of highly personal or intimate information in the discovery process triggers these rights. These privacy rights compel courts to balance privacy interests with the need to know.²⁷⁸ In divorce and custody cases, where there are requests for disclosure of intercepted conversations or stored e-mail and voicemail in the discovery process, this constitutionally based informational privacy right may be utilized to preclude innocent conversations or communications from access in discovery.

State and federal discovery rules also provide for privacy rights that would restrict discovery of innocent conversations or communications in divorce and custody cases. Under Rule 26(c) of the Federal Rules of Civil Procedure courts are authorized to limit discovery and provide protective orders, when data sought would cause unreasonable "annoyance, embarrassment, oppression or undue burden."²⁷⁹ State discovery rules generally track Rule 26(c).²⁸⁰ While the language in Rule 26(c) and analogous state rules do not specifically mention privacy, it is clear that serious invasions of privacy are

276. *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977).

277. For a general discussion of constitutionally based privacy right theory and balancing of interest test, see Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479, 487-509 (1990) and Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 136-47 (1991).

278. See Kreimer, *supra* note 277, at 146-47; Turkington, *supra* note 277, at 508-09.

279. FED. R. CIV. P. 26(c).

280. See *Rasmussen v. S. Fla. Blood Serv., Inc.*, 500 So. 2d 533, 535 (Fla. 1987); *Stenger v. Lehigh Valley Hosp. Ctr.*, 609 A.2d. 796, 799 n.6 (Pa. 1992).

included.²⁸¹ The availability of a protective order under discovery rules to protect privacy is determined by balancing privacy interests with the need to know, very much like the balancing test under the constitutional right to privacy discussed above.²⁸²

VII. CONCLUSION

Use of electronic technology to capture conversations or images and to access e-mail or voicemail is not uncommon in marriage and custody disputes between married persons and parents. Surreptitious use of this technology invades the privacy of the non-consenting party. Assessing the legality of these activities is complicated because a variety of legal institutions are implicated. This article has primarily examined whether electronic surveillance in domestic disputes violates federal and state stored communications and wiretap acts and the common law privacy intrusion tort. Wiretap acts generally restrict surreptitious recording of conversations with two limited exceptions. A minority of courts allow spouses to record conversations of other spouses on the extension phone in the marital home. There is greater authority to record conversations of a minor child on the extension phone in the home. Recently, a potentially more expansive third exception has been adopted by almost all of the courts that have considered it. This exception would authorize parents to vicariously consent to a wiretap on behalf of their minor child if the parent believes it is in the child's best interest. If the vicarious consent rule is adopted, state and federal wiretap acts that provide a one party consent defense are not violated.

The vicarious consent doctrine should be rejected primarily for two reasons: (1) the intercepting spouse is not sufficiently accountable for invasions of privacy to a non-consenting third party who is conversing with the child and (2) the vicarious consent doctrine is incomprehensible in view of state joint custody laws.

Access to e-mail and voicemail is primarily regulated by state and federal stored communications acts. This is a developing area of law and there are few appellate court decisions that construe the stored communications acts in domestic conflict cases. The clear trend is to find these statutes not applicable because e-mail stored in the home is not "in electronic storage." Beyond that, even if stored communications acts are violated, the fruits of such illegality may still be admitted in civil court proceedings because, unlike wiretap acts, stored communications acts do not contain an exclusionary rule.

281. See *Rasmussen*, 500 So. 2d at 535; *Stenger*, 609 A.2d at 803.

282. Some courts view the constitutionally based privacy right to be incorporated into the limitations on privacy contained in Rule 26(c) and analogous state discovery rules. See *Farnsworth v. Procter & Gamble Co.*, 758 F.2d 1545, 1547 (11th Cir. 1985); *Rasmussen*, 500 So. 2d at 535; *Stenger*, 609 A.2d at 803.

Electronic surveillance in domestic conflicts may be tortious under the common law privacy intrusion tort. This tort fills a void because it would reach silent video surveillance, an activity that is not regulated under wiretap and stored communications acts. In the examination of privacy intrusion tort cases, it is clear that surreptitious audio and video surveillance in domestic conflict cases may constitute tortious conduct even if the conduct does not violate wiretap and stored electronic communications acts. When analyzing such cases, one should examine the extent to which parties may have reasonable expectations of privacy in conversations and communications within the meaning of the privacy intrusion tort. In addition, it would be tortious for a spouse to access e-mail stored in a home computer if the e-mail is stored in a segregated e-mail account and the parties have maintained separate private passwords.

Much of the evidence that is obtained by illegal electronic surveillance may be admissible in marriage and custody proceedings because violations of stored electronic communications acts and the privacy intrusion tort do not provide a basis for excluding evidence in civil court proceedings. Protective orders based upon discovery rules and constitutional privacy rights may provide a way to protect privacy by excluding some communications or images from admissibility in judicial records.